☑ 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

2019년 사이버(보안)수사
시스템네트워크보안

-2019년 8월 10일 시행

1. ○△× 19.사이버

보안에 취약한 인터넷 응용 프로토콜/프로그램과 보안이 강화된 프로토콜/프로그램을 짝지은 것으로 가장 적절하지 않은 것은?

① TELNET – SSH
② SMTP – PGP
③ HTTP – HTTPS
④ FTP – TFTP

TFTP

◦ TFTP(Trivial File Transfer Protocol)는 자체 디스크를 가지고 있지 않은 시스템(예, X-터미널 등)이 부팅 시에 필요한 자료와 정보를 받아오기 위해서 사용하는 응용 프로토콜이다.

◦ 이 프로토콜의 특징은 UDP 69번을 사용하며 아무런 인증과정 없이 서버로부터 자료를 받아 올 수 있게 해준다는 것이다.

오답피하기 ④ FTP(File Transfer Protol)는 인터넷 상의 컴퓨터들 간에 파일을 교환하기 위한 표준 프로토콜이고, 이를 간단하게 만든 것이 TFTP이다. 즉 TFTP는 FTP의 보안강화와는 거리가 멀다.

정답 ④

2. ○△× 19.사이버

대표적인 스마트폰 운영체제는 iOS와 Android이다. iOS가 Android에 비해 상대적으로 안전하다고 알려져 있다. 〈보기〉 중 그 이유로 적절한 것을 모두 고른 것은?

보기

㉠ iOS는 샌드박스(sandbox)를 활용하나 Android는 그렇지 않다.
㉡ 애플은 자신의 CA(Certification Authority)를 통해 응용 프로그램을 서명하여 배포한다.
㉢ iOS는 커널 무결성 확인 후, 이상이 없으면 정상 부팅된다.
㉣ iOS는 리눅스 커널을 기반으로 만들어진 운영체제이다.

① ㉠㉡
② ㉡㉢
③ ㉡㉣
④ ㉠㉣

iOS와 안드로이드의 보안 체계 비교

구분	iOS	안드로이드
운영체제	Darwin UNIX에서 파생하여 발전한 OS X의 모바일 버전	리눅스 커널(2.6.25)을 기반으로 만들어진 모바일 운영체제
보안 통제권	애플	개발자 또는 사용자
프로그램 실행권한	관리자(root)	일반 사용자
응용 프로그램에 대한 서명	애플이 자신의 CA를 통해 각 응용프로그램을 서명하여 배포	개발자가 서명
샌드박스	엄격하게 프로그램 간 데이터 통신 통제	iOS에 비해 상대적으로 자유로운 형태의 애플리케이션의 실행이 가능
부팅 절차	암호화 로직으로 서명된 방식에 의한 안전한 부팅 절차 확보	–
소프트웨어 관리	단말 기기별 고유한 소프트웨어 설치 키 관리	–

오답피하기 ② ㉠ iOS와 Android 모두 샌드박스(sandbox)를 활용한다. ㉣ iOS는 Darwin UNIX에서 파생하여 발전한 OS X의 모바일 버전으로 만들어진 운영체제이다.

정답 ②

3. ○△× 19.사이버

패스워드에 관한 설명 중 가장 적절하지 않은 것은?

① 사용자에게 부여된 권한(authorization)을 결정한다.
② 보안 강화를 위해 주기적인 패스워드 변경이 권장된다.
③ 패스워드 보안을 위해 패스워드와 솔트(salt)를 결합한 후, 그 해시 값을 저장하는 방법이 일반적으로 사용된다.
④ 사용자는 공격자의 패스워드 추측을 어렵게 하기 위해 컴퓨터 생성 패스워드를 이용할 수 있다.

오답피하기 ① 패스워드는 주체의 신원을 검증(verify, prove)하는 인증(Authentication)에 사용된다.

정답 ①

4. ○△× 19.사이버

ARP(Address Resolution Protocol)에 관한 설명 중 가장 적절한 것은?

① ARP는 MAC 주소에 대응되는 IP 주소를 구할 때 사용되는 프로토콜이다.
② ARP 요청 메시지와 ARP 응답 메시지는 LAN 상으로 브로드캐스트 된다.
③ 호스트의 ARP 테이블을 정적(static)으로 유지하면 ARP 스푸핑 공격을 막을 수 있다.
④ ARP 패킷은 IP 데이터그램의 페이로드(payload)로 전달된다.

◦ ARP(Address Resolution Protocol, 주소 결정 프로토콜): IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜이다. 사용자는 IP 주소를 이용하여 인터넷과 연결하지만 이더넷상에서는 이더넷 주소를 이용하게 된다. 이를 위하여 IP 주소를 이더넷 주소로 변환시켜 주어야 하는데 이와 같이 IP 주소를 물리적 주소로 변환시키는 프로토콜을 주소 결정 프로토콜(ARP)이라 한다.

오답피하기 ① ARP는 IP 주소에 대응되는 MAC 주소를 구할 때 사용되는 프로토콜이다. ② ARP 요청은 유니캐스트 되고, ARP 응답은 브로드캐스트 된다. ④ ARP 패킷은 데이터링크 프레임에 캡슐화된다.

정답 ③

5. ○△× 19.사이버

〈보기〉에서 TCP를 이용하는 네트워크 공격에 해당하는 것들을 모두 고른 것은?

보기

㉠ SYN flooding 공격 ㉡ Ping of Death 공격
㉢ Telnet Session Hijacking 공격
㉣ HTTP GET flooding 공격
㉤ Smurf 공격 ㉥ ICMP Redirecting 공격

① ㉠㉡㉢
② ㉠㉢㉣
③ ㉢㉣㉤
④ ㉢㉤㉥

Telnet 세션 하이재킹

◦ 공격자는 클라이언트와 서버 간의 패킷을 중개하는 과정에서 패킷을 스니핑 하다가 Telnet 세션을 하이재킹할 수 있고, 로그인 되어져 있는 상태에서 추가적인 인증과정 없이 Telnet 서버를 장악하여 마치 공격자 자신이 직접 로그인한 것처럼 서버 내의 각종 정보를 해킹할 수 있게 된다.
◦ 이때 클라이언트는 더 이상 서비스가 지속되지 않지만 일시적으로 연결 장애가 발생한 것으로 오인하고 서버로 연결을 재설정하여 새로운 세션을 성립시켜 서비스를 받게 된다.

오답피하기 ② ㉡, ㉤, ㉥은 모두 ICMP 프로토콜과 관련되어 있다.

정답 ②

6. ○△× 19.사이버

〈보기〉의 주소들이 속해 있는 주소 블록들의 네트워크 주소와 브로드캐스트 주소가 올바르게 짝지어진 것은?

보기

㉠ 14.12.62.8/24 ㉡ 200.107.26.17/18

	㉠		㉡	
	네트워크 주소	브로드캐스트 주소	네트워크 주소	브로드캐스트 주소
①	14.12.62.0/24	14.12.62.255/24	200.107.0.0/18	200.107.63.255/18
②	14.12.62.1/24	14.12.62.255/24	200.107.1.0/18	200.107.1.255/18
③	14.12.62.0/24	14.12.62.255/24	200.107.26.0/18	200.107.26.255/18
④	14.12.62.1/24	14.12.62.255/24	200.107.192.0/18	200.107.192.255/18

오답피하기 ① IPv4에서 14.12.62.8/24 주소는 24비트까지 네트워크 주소이고 나머지 8비트는 호스트에 할당된다. 즉 네트워크 주소는 14.12.62.**0000 0000(0)**이고, 브로드캐스트 주소는 14.12.62.**1111 1111(255)**이다. 200.107.26.17(**200.107.00**00 1110.17)/18 주소는 18비트까지 네트워크 주소이고 나머지 14비트는 호스트에 할당된다. 즉 네트워크 주소는 **200.107.00**00 0000.0000 0000(200.107.0.0)이고, 브로드캐스트 주소는 200.107.00**11 1111.1111 1111**(200.107.63.255)이다.

정답 ①

7. ○△× 19.사이버

〈보기 1〉의 용어와 〈보기 2〉의 설명을 연결한 것으로 가장 적절한 것은?

보기1

(가) Footprinting
(나) APT(Advanced Persistent Threat) 공격
(다) Promiscuous 모드
(라) Zero Day 공격

보기2

㉠ 특정 기업 또는 기관의 시스템을 목표로 한 장기적이고 정교한 공격
㉡ 컴퓨터 소프트웨어의 취약점에 대한 패치가 나오지 않은 시점에 이루어지는 공격
㉢ 해킹하기 전에 공격 대상에 대한 정보를 모으는 사전 준비 작업
㉣ 스니핑을 위해 랜카드의 필터링 기능을 해제

	(가)	(나)	(다)	(라)
①	㉠	㉡	㉢	㉣
②	㉡	㉠	㉣	㉢
③	㉢	㉠	㉣	㉡
④	㉣	㉡	㉢	㉠

◦ 풋프린팅(Footprinting): 해킹 시도 대상의 관련 정보를 수집하는 사전 작업이다.
◦ 지능형 지속 위협(APT, Advanced Persistent Threats): 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 정보를 외부로 빼돌리는 형태의 공격이다.
◦ 무차별 모드(Promiscuous Mode): 원래 NIC는 기본적으로 자기의 MAC 주소와 일치하거나, Broadcast 패킷만 받도록 설정되어 있다. 그런데, 스니퍼를 실행하게 되면 자신의 NIC는 아무거나 받아들이게 된다. 이러한 모드를 Promiscuous mode라고 한다. 만약 자신의 시스템의 NIC가 Promiscuous mode로 동작한다면 스니퍼가 실행된다고 생각하면 된다.
◦ 제로데이공격(Zero-Day Attack): 해킹에 악용될 수 있는 시스템 취약점에 대한 보안패치가 발표되기 전에, 이 취약점을 악용해 악성코드를 유포하거나 해킹을 시도하는 것을 말한다. 보안패치가 나오기 전까지는 이를 근본적으로 막을 수 없다는 점에서 가장 우려되는 공격 형태이다.

오답피하기 ③ 보안에서 자주 사용하는 용어로 반드시 숙지해야 한다.

정답 ③

8. ○△× 19.사이버

다음 표는 패킷 필터링 방화벽에 적용된 필터링 규칙의 예이다. 표에 대한 설명 중 가장 적절하지 않은 것은? (방화벽은 내부 네트워크와 외부 네트워크의 경계에 위치하는 것으로 가정함)

규칙	방향	발신지 IP주소	목적지 IP주소	프로토콜	목적지 포트번호	동작
A	안으로	외부	내부	TCP	25	허용
B	밖으로	내부	외부	TCP	25	허용
C	안으로	외부	내부	TCP	80	허용
D	양방향	전부	전부	TCP/UDP	전부	거절

① 방화벽 내부의 사용자들은 외부로 전자메일을 전송할 수 있다.
② 방화벽 내부의 사용자들은 외부의 FTP 서버에 접속할 수 없다.
③ 방화벽 내부의 사용자들은 외부의 웹 서버에 접속할 수 있다.
④ 방화벽 내부의 사용자들은 외부의 텔넷 서버에 접속할 수 없다.

① 방화벽 내부의 사용자들은 외부로 전자메일을 전송할 수 있다. – 규칙 B 적용
② 방화벽 내부의 사용자들은 외부의 FTP 서버에 접속할 수 없다. – 규칙 D 적용
④ 방화벽 내부의 사용자들은 외부의 텔넷 서버에 접속할 수 없다. – 규칙 D 적용

오답피하기 ③ 방화벽 내부의 사용자들은 외부의 웹 서버에 접속할 수 있다. – 규칙 C는 방향이 안으로(외부 → 내부)이므로 적용이 안 되어 패스되고, 규칙 D의 적용을 받아 거절된다.

정답 ③

9. ○△× 19.사이버

〈보기〉의 NAT(Network Address Translation) 라우터에 대한 설명으로 옳은 것을 모두 고른 것은?

보기

㉠ 사설 IP주소와 공인 IP주소의 매핑을 제공한다.
㉡ NAT 라우터는 일반적으로 IP주소와 포트 번호를 조합하여 매핑한다.
㉢ IPv4 주소 고갈 문제를 완화할 수 있으며 보안 상 이점을 갖는다.
㉣ 사설망 내부에서 웹 서버 운영 시 port forwarding을 통해 접속을 허용할 수 있다.

① ㉠㉢
② ㉠㉡㉢
③ ㉠㉢㉣
④ ㉠㉡㉢㉣

◦ 포트 포워딩(port forwarding) : 컴퓨터에서 특정 통신 포트를 개방하여 통신이 되도록 하는 것이다. 예를 들어 내부 포트를 외부 원격 서버에 전달되도록 지정하거나, 방화벽을 그대로 유지하면서 방화벽의 특정 포트를 내부망의 특정 호스트와 연결시킨다. 마이크로소프트 윈도우 XP 서비스 팩 2에 들어간 윈도우 방화벽을 비롯한 대부분의 방화벽 소프트웨어, 인터넷 공유기는 포트 포워딩 메뉴가 있고, 여기에 개방할 포트 번호를 등록하여 사용할 수 있다.

오답피하기 ④ 네트워크 주소 변환(NAT)은 사설 주소와 범용(공인) 주소의 매핑을 제공하고 동시에 가상 사설 네트워크를 지원하는 기술로, 보기는 NAT의 특징에 대한 설명이다.

정답 ④

10. ○△× 19.사이버

리눅스 시스템의 사용자 계정 관련 파일로 가장 적절하지 않은 것은?

① /etc/passwd
② /etc/shadow
③ /etc/permission
④ /etc/group

◦ /etc/passwd 파일은 개별 사용자에 대한 정보로 이루어져 있다.
◦ /etc/shadow 파일에는 계정별 암호화된 패스워드 정보와 패스워드 에이징(aging) 정보가 저장되어 있다. 패스워드 에이징 정보는 시간의 흐름에 따른 패스워드 관리정책을 말한다.
◦ /etc/group 파일은 현재 시스템에 정의되어 있는 모든 그룹의 정보를 저장하고 있다. 즉, /etc/passwd 파일에 담긴 기본 그룹(GID)의 정보는 /etc/group 파일에 정의된다.

오답피하기 ③ /etc/passwd, /etc/shadow, /etc/group 파일은 사용자 계정 관련 파일들이다. /etc/permission은 전혀 관련이 없다.

정답 ③

11. ○△× 19.사이버

네트워크 진단 프로그램에 대한 설명으로 가장 적절하지 않은 것은?

① traceroute – 지정한 호스트까지의 경로를 조사하는 프로그램
② nslookup – DNS 서버에 도메인 네임에 관한 질의를 하는 프로그램
③ metasploit – 네트워크 토폴로지를 매핑시키는 프로그램
④ tcpdump – 네트워크 패킷 캡처 프로그램

Metasploit Project

◦ 메타스플로이트 프로젝트(Metasploit Project)에서 메타스플로이트는 펄 스크립팅 언어를 사용하는 휴대용 네트워크 도구로서 2003년 H. D. 무어에 의해 만들어졌다. 그러나 루비(RUBY)에 의하여 재구조 된 이후 2009년 10월 21일 Rapid7, 통일 취약성 관리 솔루션을 제공하는 보안 회사에 인수되었고, 현재는 오픈 소스, 보안 취약점, 침투 테스트 및 IDS 서명 개발 보조기구 등에 대한 정보를 제공하는 것에 목적을 두는 컴퓨터 보안 프로젝트이다.
◦ 메타스플로이트 프레임워크는 버퍼 오버플로우, 패스워드 취약점, 웹 응용 취약점, 데이터베이스, 와이파이 취약점 등에 대한 약 300개 이상의 공격 모듈을 가지고 있는 오픈 소스 도구로서, 메타스플로이트를 이용하면 저렴한 비용으로 기업의 시스템에 대한 포괄적인 침투시험을 통해 취약성을 확인할 수 있다.

오답피하기 ③ metasploit는 모의해킹, 취약점진단 및 분석을 수행할 수 있는 도구이다.

정답 ③

12. ○△× 19.사이버

네트워크 보안 프로토콜에 대한 설명 중 가장 적절하지 않은 것은?

① EAP(Extensible Authentication Protocol)는 다양한 인증 방법을 지원하는 네트워크 접근 제어 프로토콜이다.
② IPsec(IP Security)은 AH(Authentication Header)를 통해 인증, 무결성, 기밀성을 제공한다.
③ TLS(Transport Layer Security)는 최근 버전 1.3으로

표준화되었으며, 핸드셰이크(handshake) 과정을 통해 암호화에 필요한 알고리즘 및 관련 매개변수를 교환한다.

④ DNSSEC(DNS Security)은 DNS 데이터 인증과 무결성을 보장하지만, DNS 서버에 대한 DoS(Denial of Service) 공격은 막지 못한다.

TLS 버전

- TLS 1.3은 2018년 8월에 RFC 8446으로 게시되었다.
- Chrome, Firefox, Edge, Safari, Explorer를 포함한 주요 웹 브라우저가 2020년에 TLS 1.0 및 TLS 1.1 통신에 대한 지원을 중지한다고 발표했다.
- TLS의 초기 버전인 TLS1.0, TLS1.1은 POODLE 및 BEAST와 같은 다양한 공격에 취약하다.

오답피하기 ② AH는 인증, 무결성을 제공하지만 기밀성은 제공하지 않는다. 기밀성은 ESP를 통해 제공가능하다.

정답 ②

13. ○△× 19.사이버

IEEE 802.11i에 관한 설명으로 가장 적절하지 않은 것은?

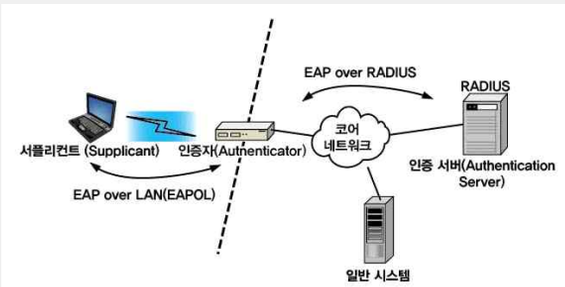
① IEEE 802.11 무선랜의 보안 표준으로 인증, 데이터 무결성, 데이터 기밀성, 키 관리에 관한 내용을 포함한다.

② 무선단말(station)과 무선접속점(access point) 간의 안전한 통신을 제공한다.

③ 인증서버(authentication server)는 무선단말을 인증한다.

④ 무선단말과 무선접속점은 RADIUS(Remote Authentication Dial In User Service) 프로토콜을 통해 인증 정보를 교환한다.

802.1x 보안



오답피하기 ④ 802.1x에서 EAP 인증 시에 사용자와 AP 사이에는 EAPOL(EAP over LAN)프로토콜을 통해서 패킷을 전송하고, AP와 인증서버 사이에는 RADIUS(Remote Authentication Dial-in User Services) 프로토콜을 통해서 패킷을 전송한다.

정답 ④

14. ○△× 19.사이버

C 언어로 개발된 소프트웨어의 메모리 오염(memory corruption)에 대한 설명으로 가장 적절하지 않은 것은?

① Heap Buffer Overflow – malloc() 함수를 통해 힙(heap) 영역에 할당한 변수의 메모리 경계를 검사하지 않고 사용할 때 발생할 수 있음

② Integer Overflow – 변수의 자료형보다 큰 수를 저장할 때 발생할 수 있음

③ Use-After-Free – free() 함수를 통해 이미 해제된 포인터를 사용할 때 발생할 수 있음

④ Double Free – free() 함수를 통해 포인터 해제 후, 같은 이름의 포인터를 생성하고 free() 함수로 해제할 때 발생할 수 있음

- 정수형 변수의 오버플로우는 정수값이 증가하면서, 허용된 가장 큰 값보다 더 커져서 실제 저장되는 값이 의도하지 않게 아주 작은 수이거나 음수가 되어 발생한다. 특히 반복문 제어, 메모리 할당, 메모리 복사 등을 위한 조건으로 사용하는 외부 입력값이 오버플로우 되는 경우 보안상 문제를 유발할 수 있다.
- Use After Free(UAF): Heap 영역은 동적으로 메모리가 할당되고 해제된다. 할당할 때는 malloc 등의 함수를 사용하고 해제할 때는 free 함수를 사용한다. UAF는 메모리 영역을 free 한 후에 동일 공간을 재사용하게 될 경우에 발생할 수 있다.

오답피하기 ④ Double Free 취약점은 동일한 값에 대해 free()를 두 번 호출할 때 발생할 수 있다. 즉 프로그램이 같은 인수로 free()를 두 번 호출하면 프로그램의 메모리 관리 데이터 구조가 손상될 수 있는 취약점이다.

정답 ④

15. ○△× 19.사이버

DEP(Data Execution Prevention)에 대한 설명으로 가장 적절하지 않은 것은?

① 실행 권한이 없는 메모리 영역에서 코드가 실행되지 않도록 하는 기법을 말한다.

② CPU에서 지원하는 하드웨어 기반 DEP과 운영체제가 지원하는 소프트웨어 기반 DEP으로 구분할 수 있다.

③ ROP(Return Oriented Programming) 기법에 의해 우회가 가능하다.

④ RTL(Return To Library) 공격을 막기 위해 개발되었다.

- 데이터 실행 방지(Data Execution Prevention, DEP)는 현대의 마이크로소프트 윈도우 운영 체제에 포함된 보안 기능이며, 실행 방지 메모리 영역의 실행 코드에서 응용 프로그램이나 서비스가 실행되지 못하게 막기 위해 고안된 것이다.
- 반환 지향형 프로그래밍(ROP: Return-oriented programming)은 실행 불가능한 메모리(NXbit)와 코드 사이닝(Code Signing) 같은 보안 방어가 존재하는 경우에 공격자가 코드를 실행할 수 있게 하는 컴퓨터 보안

취약점 공격이다.

오답피하기 ④ DEP은 힙스프레이를 방지하기 위한 방법이다. 힙스프레이는 메모리의 힙(heap) 영역에 Nop sled(아무런 동작을 하지 않는 0x90 혹은 이와 유사한 인스트럭션이 연속적으로 나오는 코드)와 셸코드의 조합을 대규모로 뿌려(spraying) ASLR(Address Space Layout Randomization) 등의 보안기술을 회피하는 기법이다. Return-into-library 기법은 rtl(return to libc)이라고도 하는데 Non-Executable Stack을 우회할 때 사용한다.

정답 ④

16. ○△× 19.사이버

32비트 인텔 CPU 아키텍처에서 윈도우 운영체제를 사용한다고 가정할 때, 어셈블리어 명령어들에 대한 설명이다. 가장 적절하지 않은 것은?

① ADD ECX, 10 – 카운터 레지스터 ECX에 10을 더한 후 데이터 레지스터 EDX에 저장
② MOV ECX, 4 – 카운터 레지스터 ECX에 4를 저장
③ INC EAX – 누산기 레지스터 EAX에 저장된 값을 1 만큼 증가
④ CALL EBX – 베이스 레지스터 EBX에 저장된 주소로 이동 및 실행

◘ 어셈블리어 언어
◦ ADD(Add): Destination에 Source의 값을 더해서 Destination에 저장하는 명령이다.
– 형식: ADD destination, source
– 예시: ADD eax, 123
/* 위 명령은 eax 레지스터에 123을 더해서 eax 레지스터에 저장한다. */
◦ SUB(Subtract): Destination에 Source의 값을 빼서 Destination에 저장하는 명령이다.
– 형식: SUB destination, source
– 예시: SUB eax, 123
/* 위 명령은 eax 레지스터에 123을 빼서 eax 레지스터에 저장한다. */
◦ CALL: CALL 명령어 다음에 오는 명령어의 주소를 스택에 PUSH하고 주어진 주소로 제어를 옮긴다.
– 형식: call Target
– 설명: 스택 상에서 명령의 오프셋 어드레스를 PUSH하고 target으로 이동한다.

오답피하기 ① ADD ECX, 10 – 카운터 레지스터 ECX에 10을 더한 후 ECX에 저장한다.

정답 ①

17. ○△× 19.사이버

백도어(backdoor)에 관한 설명으로 가장 적절하지 않은 것은?

① 백도어는 공격자에 의해 시스템 관리자 권한이 탈취된 후 설치되거나, 백도어가 이미 탑재된 악의적인 소프트웨어 설치를 통해 시스템에 설치될 수 있다.
② 하드웨어 펌웨어에 탑재된 백도어는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.
③ 운영체제 레벨의 백도어(예를 들어 악의적인 코드가 탑재된 kernel32.dll)는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.
④ 응용 레벨의 백도어는 현재 동작 중인 프로세스 확인, 포트 검사, 바이러스 탐지 툴, 시스템 무결성 검사 등으로 탐지가 가능하다.

◘ 백도어(Backdoor)
◦ 백도어(Backdoor)는 운영체제 또는 애플리케이션(프로그램)을 만들 때 정상적인 인증 과정을 무시하고 운영체제 또는 애플리케이션(프로그램)에 접근할 수 있도록 만들어 놓은 보안상의 뒷구멍이다.
◦ 백도어는 펌웨어 · 커널 · 부트로더 · 암호화 알고리즘 · 하드웨어 등 다양한 영역에 들어가 있을 수 있으며, 발견하는 데 상당히 힘들다.
◦ 백도어를 심는 이유는 장치 및 네트워크를 제어 및 감시하는 데 있다.

오답피하기 ② 하드웨어 펌웨어에 탑재된 백도어는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 없다.

정답 ②

18. ○△× 19.사이버

암호 알고리즘에 대한 설명 중 가장 적절하지 않은 것은?

① AES는 기존 DES, 3DES의 취약한 암호 강도를 극복하고자 미국 NIST에서 전세계 암호학자들에게 공모를 통하여 선정한 비대칭 암호 알고리즘으로 데이터에 대한 기밀성 및 부인 방지 기능을 제공한다.
② RC5는 미국 RSA 연구소에서 개발한 입출력, 키, 라운드 수가 가변적인 블록 암호 알고리즘으로 DES에 비해 빠른 연산 속도를 제공한다.
③ SEED는 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 블록 암호 알고리즘이며, 국제표준화기구인 ISO/IEC와 IETF로부터 암호 표준 알고리즘으로 인정받았다.
④ ARIA는 국가보안기술연구소와 국내 암호 전문가들이 경량 환경을 위해 개발한 블록 암호 알고리즘이다.

◘ RC5
◦ 1994년 미국 RSA 연구소의 라이베스트(Rivest)가 개발한 것으로 비교적 간단한 연산으로 빠른 암호화와 복호화 기능을 제공하며, 모든 하드웨어에 적합하다.

◦ 입출력, 키, 라운드 수가 가변인 블록 알고리즘 RC5(Ron's Code 5)는 32/64/128/비트의 블록을 가지며, 속도는 DES의 약 10배이다.

오답피하기 ① AES는 대칭키 알고리즘으로 데이터에 대한 기밀성을 제공한다.

정답 ①

19. ○△× 19.사이버

다음 설명 중 가장 적절하지 않은 것은?

① 워터마크(watermark)는 저작권 보호를 위해 이미지나 동영상 파일에 저작권 정보를 삽입하는 기법을 말한다.
② DRM(Digital Right Management)은 문서나 동영상 파일에 보안성을 제공하기 위해 암호화 하고 인가된 사용자에 한해서 해당 파일에 접근할 수 있는 권한을 부여한다.
③ 백신 프로그램은 문서나 동영상에 접근할 수 없는 사용자로부터 해당 파일의 저작권을 보호한다.
④ 방화벽은 워터마크나 DRM이 적용된 파일을 탐지하지 못한다.

◦ 백신 프로그램(vaccine program)은 컴퓨터 바이러스 프로그램을 찾아내고 손상된 파일을 치료하는 소프트웨어이다. 특정 파일에 대한 기록이나 변경을 감시하거나 주기적 덧붙임 검사(CRC) 등을 통해 바이러스 감염 여부를 검사한 후에 침범한 바이러스를 제거한다.

오답피하기 ③ 백신 프로그램은 파일의 저작권 보호와는 관련이 없다.

정답 ③

20. ○△× 19.사이버

다음 설명 중 가장 적절하지 않은 것은?

① 비트코인(Bitcoin)은 블록체인(blockchain) 기반 암호화폐(cryptocurrency)이다.
② 비트코인은 공개키 기반 주소를 사용하고 트랜잭션(transaction)을 암호화하여 전송하기 때문에 익명성이 보장된다.
③ 비트코인 블록체인의 작업증명(Proof-of-Work)은 단방향 해시 함수의 특성을 이용한다.
④ 비트코인 블록체인은 누구나 참여할 수 있는 공개형 블록체인이다.

◦ 작업증명(PoW, Proof of Work) : 최초의 블록체인인 비트코인을 창시한 사토시 나카모토가 제안한 합의 알고리즘이다. 새로 만든 블록을 앞 블록에 연결하는데 필요한 해시를 만들고 해시 연결성을 검증하여 데이터가 중간에 위변조가 되지 않았음을 확인한다.
◦ 누구나 참여할 수 있는 블록체인을 퍼블릭 블록체인이라고 하는데, 이는 퍼미션리스(permissionless) 블록체인 혹은 비허가형(공개형) 블록체인이라고 불린다. 말 그대로 블록체인을 유지·관리하는 합의 과정에 누구나 참여할 수 있는 시스템을 말한다. 대표적으로는 비트코인이나 이더리움 등이 있다.

오답피하기 ② 비트코인은 공개키 암호, 전자서명 그리고 해시함수 등의 암호기술을 사용하지만 공개키 기반 주소는 사용하지 않는다. 그러나 거래 당사자들에 대한 정보가 연결되어 있지 않아 소유자에 대한 정보는 알 수 없으므로 익명성은 보장된다.

정답 ②

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