

# 2016년도 제1회 국민안전처 소속 일반직공무원(9급) 채용시험 문제지

과 목	네트워크보안	응시번호	성 명
1. 다음 중 물리계층 프로토콜과 관계가 가장 먼 것은? ① RS-232C                              ② i430 ③ X.25                                      ④ RS-449		7. <보기>의 설명에 해당하는 네트워크 장비는? <div>&lt; 보기 &gt; · OSI계층 모델의 네트워크 계층에서 동작하는 장비이다. · 송신측과 수신측 간의 가장 빠르고 신뢰성 있는 경로를 설정·관리하며, 데이터를 전달하는 역할을 한다. · 주로 같은 프로토콜을 사용하는 네트워크간의 최적경로 설정을 위해 패킷이 지나가야 할 정보를 테이블에 저장하여 지정된 경로를 통해 전송한다.</div> ① 게이트웨이(gateway)                      ② 브리지(bridge) ③ 리피터(repeater)                              ④ 라우터(router)	
2. 다음 지문에서 설명하고 있는 것은 무엇인가? <div>침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상 사설망(VPN) 등 서로 다른 보안제품에서 발생하는 정보를 한 곳에서 모으는 역할을 하는 보안관제 시스템</div> ① ESM                                      ② NMS ③ TMS                                      ④ IPS		8. 가설사설망(VPN)이 제공하는 보안 서비스에 해당하지 않는 것은? ① 패킷 필터링                                      ② 데이터 암호화 ③ 접근제어    ④ 터널링	
3. 다음에서 허니팟(honeypot)이 갖는 고유 특징에 대한 설명으로 옳지 않은 것은? ① 공격자의 행동 패턴에 대한 유용한 정보를 수집할 수 있다. ② 중요한 시스템을 보호하기 위해서 잠재적 공격자를 유혹한다. ③ 시스템을 관찰하고 침입을 방지할 수 있는 규칙이 적용된다. ④ 대응책을 강구하기에 충분한 시간 동안 공격자가 머물게 한다.		9. 무선랜 보안 방식인 WEP(Wired Equivalent Privacy)은 일정한 양의 데이터를 분석하면 이로부터 키(key)를 추출할 수 있는 단점이 발견되었다. 802.11i에서 WEP 보다 강화된 보안 방식인 WPA 및 WPA2를 제안하는데 개인용은 인증을 위해 어떤 방식을 사용하는지 고르시오. ① 802.11x ② AES(Advanced Encryption Standard) ③ TKIP(Temporary Key Integrity Protocol) ④ PSK(Pre-Shared Key)	
4. 서비스 거부 공격 방법이 아닌 것은? ① ARP spoofing                              ② Smurf ③ SYN flooding                              ④ UDP flooding		10. 회선 교환 방식은 정보전송의 필요성이 생겼을 때 상대방을 호출하여 물리적인 연결을 구성한 후 정보를 전송하는 방식을 말한다. 다음 중에서 회선 교환 방식의 특징이 아닌 것은? ① 항상 동일한 경로를 이용하여 전송한다. ② 대체적으로 Point-to-Point의 전송구조를 갖는다. ③ 경로 설정에 짧은 시간이 걸리며 전송지연이 거의 없다. ④ 고정적인 대역폭을 사용한다.	
5. 스니핑(sniffing)을 방지하기 위한 대책으로 옳바르지 못한 것은? ① 스위치 포트에 접근 제한을 설정한다. ② 전자메일을 이용할 때에는 IPSec 기술을 사용하여 암호화 한다. ③ 원격 접속 프로그램으로는 telnet 대신 ssh 프로토콜을 이용한다. ④ VPN을 이용하여 네트워크 구간을 암호화 한다.		11. CIDR을 지원하는 라우팅 프로토콜이 아닌 것은? ① RIPv1    ② OSPF ③ BGP-4    ④ IS-IS	
6. 안드로이드 보안에 대한 설명으로 옳지 않은 것은? ① 리눅스 운영체제와 유사한 보안 취약점을 갖는다. ② 개방형 운영체제로서의 보안정책을 적용한다. ③ 응용프로그램에 대한 전자서명은 개발자가 한다. ④ 응용프로그램 간 데이터 통신을 엄격하게 통제한다.			

2016년도 제1회 국민안전처 소속 일반직공무원(9급) 채용시험 문제지

과 목	네트워크보안	응시번호	성 명
12. 최근 많이 발생하는 공격 사례로 인터넷 사용자의 컴퓨터에 침입하여 내부 문서나, 사진파일, 스프레드 시트 등 사용자의 파일들을 암호화하여 파일을 열지 못하도록 한 뒤 돈을 보내주면 암호화를 풀 수 있는 프로그램을 전송해 준다며 금품을 요구하는 악성프로그램을 뜻한다. 이러한 공격을 무엇이라고 하는가?	16. 이더넷(Ethernet) MAC(Media Access Control) Address를 정의하는 표준 Format은 몇 비트인가?		
① 랜섬웨어(Ransomware)	① 8bit		
② APT(Advanced Persistent Threat)	② 16bit		
③ DDoS(Distributed Denial of Service)	③ 48bit		
④ 스미싱(Smishing)	④ 64bit		
13. 침입차단시스템 방식 중에 어플리케이션 게이트웨이방식 설명으로 옳지 않은 것은?	17. 다음 지문은 무엇에 대한 설명인가?		
① 외부 네트워크와 내부 네트워크가 프록시 서버를 통해야만 연결이 된다.	패킷이 목적지까지 도달하는 동안 거치는 라우터 IP를 확인하는 도구이다. 이 도구는 udp와 icmp, ip의 ttl값을 이용한다. 명령어에 대한 결과에서 응답시간이 *로 표시되는 경우 침입차단시스템 등의 접근통제리스트에 의해 패킷이 차단되었음을 확인할 수 있다.		
② 내부 네트워크에 대한 경계선 방어 및 내부 네트워크에 대한 정보를 숨길 수 있다.	① traceroute		
③ 패킷 필터링 방화벽보다 높은 보안성 설정이 가능하다.	② ping		
④ 하나의 프록시 데몬이 존재한다.	③ netstat		
14. 다음 설명에 해당하는 컴퓨터 바이러스는?	④ route		
산업 소프트웨어와 공정 설비를 공격 목표로 하는 극도로 정교한 군사적 수준의 사이버 무기로 지칭된다. 공정 설비와 연결된 프로그램이 논리제어장치(Programmable Logic Controller)의 코드를 악의적으로 변경하여 제어권을 획득한다. 네트워크와 이동저장매체인 USB를 통해 전파되며, SCADA(Supervisory Control and Data Acquisition) 시스템이 공격 목표이다.	18. 다음 중 침입탐지시스템(IDS)의 주요기능이 아닌 것은?		
① 오토런 바이러스(Autorun virus)	① 데이터 수집(Raw Data Collection)		
② 백도어(Backdoor)	② 데이터 축약과 필터링(Data Reduction and Filtering)		
③ 스텝스넷(Stuxnet)	③ 침입분석 및 탐지(Analysis and Intrusion Detection)		
④ 봇넷(Botnet)	④ 역추적(Back Trace)		
15. TCP와 UDP를 비교한 것 중 잘못된 것은 ?	19. 다음 중 IPv6의 전달 방식 중 애니캐스트(AnyCast)에 대한 설명으로 가장 바른 것은?		
① UDP는 비연결형 서비스이고, TCP는 연결형 서비스이다.	① 하나의 호스트에서 다른 하나의 호스트에게 전달하는 방식		
② TCP는 수신순서가 데이터의 송신순서와 동일하지만, UDP는 송신순서와 다를 수 있다.	② 하나의 호스트에서 그룹 내의 가장 가까운 곳에 있는 수신자에게 전달하는 방식		
③ TCP는 바이트 스트림 단위로, UDP는 블록단위로 비트정보를 전송한다.	③ 다중호스트를 여러 개의 호스트들에게 전달하는 방식		
④ TCP와 UDP는 오류제어와 흐름제어 기능을 수행한다.	④ 하나의 호스트에서 모든 호스트들에게 전달하는 방식		
	20. 악성코드를 운반하는 페이로드(payload)의 네 가지 분류와 예가 잘못 연결된 것은?		
	① 시스템 파괴 - 논리폭탄, Stuxnet		
	② 공격 에이전트 - 랜섬웨어, 트랩 도어		
	③ 정보 유출 - 키로거, 피싱, 스파이웨어		
	④ 잠입 - 백도어, 루트킷		