

네트워크보안

2018년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. IP 동작을 진단하거나 제어하는 데 사용되는 ICMP(Internet Control Message Protocol)에 대한 다음 물음에 답하시오. (총 20점)

- 1) ICMP 패킷의 구조에 대해 설명하시오. (5점)
- 2) ICMP 메시지는 오류 보고 메시지와 질의 메시지로 분류된다. 이 중 오류 보고 메시지들의 타입과 기능에 대해 설명하시오. (5점)
- 3) ICMP를 이용하여 공격 대상 시스템의 서비스가 활성화 되었는지 알아보는 방법에 대해 설명하시오. (10점)

제 2 문. 서비스 거부(Denial of Service) 공격에 활용되는 SYN Flooding에 대한 다음 물음에 답하시오. (총 20점)

- 1) 정상적인 TCP 3단계 핸드셰이킹(three-way handshaking) 과정을 순서번호(sequence number)와 확인응답번호(acknowledgement number)를 포함하여 설명하시오. (5점)
- 2) SYN Flooding 공격 과정을 단계별로 설명하시오. (5점)
- 3) SYN Flooding 공격에 대한 대응 방안들에 대해 설명하시오. (10점)

제 3 문. 인터넷 사용자의 단말은 도메인 이름에 해당하는 IP 주소를 얻기 위해서, 일반적으로 네트워크 서비스 업체나 소속 기관이 운영하는 로컬 DNS 서버를 이용한다. 다음 물음에 답하시오. (총 24점)

- 1) 사용자 단말이 특정 도메인 이름에 대한 IP 주소를 로컬 DNS 서버에 질의 하였을 때, 로컬 DNS 서버가 이에 대한 정보를 가지고 있지 않다고 가정한다. 로컬 DNS 서버가 최종적으로 특정 도메인의 DNS 서버로부터 IP 주소를 얻어 오는 과정을 설명하시오. (6점)
- 2) 공격자가 사용자 단말로부터 발생된 DNS 질의를 가로채고 로컬 DNS 서버가 응답하기 전에 대신 응답하는 방식의 DNS 스푸핑 공격 시, 로컬 DNS 서버가 보낸 것처럼 위장하기 위하여 응답 패킷의 헤더 정보를 조작하는 방법을 설명하시오. (8점)
- 3) DNS 캐시 포이즈닝(cache poisoning)의 방법과 위험성을 설명하시오. (10점)

제 4 문. 동일한 무선 매체에 접근하려고 경쟁하는 무선 지국(STA: Station)들로 구성되는 기본 서비스 집합(BSS: Basic Service Set)의 AP(Access Point)들이 연결된 분산 시스템이 주어져 있을 때, 무선 랜(LAN) 보안 표준인 IEEE 802.11i에 대한 다음 물음에 답하시오. (총 36점)

- 1) 전체 시스템 중 IEEE 802.11i가 관여하는 안전한 통신 구간에 대해 설명하시오. (6점)
- 2) STA와 인증 서버(AS: Authentication Server) 간의 상호 인증 절차를 설명하고, 이러한 상호 인증 절차를 통해 얻어지는 이점을 설명하시오. (10점)
- 3) 사용자 트래픽에 대한 실질적 보호에 사용되는 키가 얻어지는 과정을 설명하시오. (10점)
- 4) IEEE 802.11 MPDU(MAC Protocol Data Unit)를 전달하기 위한 두 가지 보안 프로토콜과 각 프로토콜이 제공하는 보안 서비스에 대해 설명하시오. (10점)

인사혁신처 시험출제과장