

## 네트워크보안

### 2016년 시행 5급 공채(기술) 제2차시험

응시번호 :

성명 :

제 1 문. 서버와 클라이언트, 공격자의 IP 주소가 각각 192.168.0.1, 192.168.0.2, 192.168.0.3이고, MAC 주소도 순서대로 aa:aa:aa:aa:aa:aa, bb:bb:bb:bb:bb:bb, cc:cc:cc:cc:cc:cc로 주어진다고 가정할 때, 다음 물음에 답하시오. (총 25점)

- 1) 공격자가 ARP 스누핑을 이용하여 서버와 클라이언트 간의 통신을 스니핑(sniffing)하는 절차를 설명하시오. (15점)
- 2) 1)에서의 스니핑에 대응할 수 있는 방법을, ARP Table을 대상으로 하는 것과 그렇지 않은 것으로 구분하여 설명하시오. (10점)

제 2 문. IPSec(IP Security)은 IP 계층의 패킷 트래픽을 인증하고 암호화한다. 다음 물음에 답하시오. (총 30점)

- 1) IPSec을 구성하는 AH(Authentication Header) 프로토콜과 ESP(Encapsulating Security Payload) 프로토콜이 제공하는 보안 서비스를 각각 설명하시오. (9점)
- 2) TCP 세그먼트를 포함하는 IPv4 패킷이 ESP 프로토콜의 터널 모드(Tunnel mode)를 통해 전송될 경우, 변경된 패킷 구조와 추가된 필드의 기능을 설명하시오. (12점)
- 3) 트랜스포트 모드(Transport mode) ESP에 비해 터널 모드(Tunnel mode) ESP의 장점을 설명하시오. (9점)

제 3 문. 무선랜의 보안 프로토콜인 WEP(Wired Equivalency Protocol)는 RC4 스트림 암호 알고리즘을 사용하여 데이터의 기밀성과 무결성을 보장한다. WEP 프로토콜 송신자가 다음과 같은 방법으로 MAC 계층 데이터 유닛을 구성할 때, 다음 물음에 답하시오. (총 25점)

- i. 송신자는 초기 벡터값 IV(Initialization Vector)를 선택한다.
- ii. 송·수신자 양쪽이 공유하는 비밀키 뒤에 IV 값을 붙여 RC4 키를 생성한다.
- iii. 전송할 데이터 블록의 CRC(Cyclic Redundancy Check) 값을 구하여 데이터 블록 뒤에 붙인다.
- iv. 데이터 블록과 CRC 값 전체를 RC4 키로 암호화하고, 암호문 앞에 IV 값을 붙인다.

- 1) 수신자가 암호문으로부터 평문을 복구하고 데이터의 무결성을 검증하는 방법을 설명하시오. (15점)
- 2) 송신자가 IV 값을 다시 사용할 때 발생될 수 있는 문제를 설명하시오. (10점)

제 4 문. HTTPS에 대한 Heartbleed 공격 등이 증가함에 따라 완전 순방향 비밀성(Perfect Forward Secrecy)을 보장하는 보안 프로토콜의 필요성이 높아지고 있다. 다음 물음에 답하시오. (총 20점)

- 1) 완전 순방향 비밀성의 개념을 설명하시오. (10점)
- 2) TLS에서 Diffie-Hellman 키교환을 기반으로 완전 순방향 비밀성을 보장하는 방법을 설명하시오. (10점)

## 인사혁신처 시험출제과장