

네트워크보안

2019년도 국가공무원 5급(기술) 공개경쟁채용 제2차시험

응시번호 :

성명 :

제 1 문. DRDoS(Distributed Reflection DoS) 공격에 대한 다음 물음에 답하시오.
(총 25점)

- 1) TCP의 연결설정과정(3way-handshake)의 취약점을 이용한 DRDoS의 공격 절차를 3단계로 나누어 순서대로 기술하시오. (15점)
- 2) 일반 DoS 공격과의 차이점을 2가지 설명하시오. (10점)

제 2 문. 네트워크에서 DMZ(DeMilitarized Zone)에 대한 다음 물음에 답하시오.
(총 26점)

- 1) DMZ를 구축하는 목적을 기술하시오. (4점)
- 2) DMZ 영역에 위치하는 대표적 서비스를 3가지 이상 기술하시오. (6점)
- 3) 방화벽의 대표적 유형 4가지를 그림과 함께 설명하시오. (16점)

제 3 문. 최근 불법음란물을 유포하는 사이트가 사회적으로 문제가 되고 있다. 이와 관련하여 다음 물음에 답하시오. (총 20점)

- 1) 웹서비스를 크게 Surface web, Dark web, Deep web으로 구분할 수 있다. 이를 각각 설명하시오. (6점)
- 2) Dark web에 접속하기 위한 대표적 브라우저는 무엇이며, Dark web 서비스를 받기 위한 클라이언트부터 서버까지의 통신과정을 설명하시오. (14점)

제 4 문. 침입탐지시스템(IDS)에 대한 다음 물음에 답하시오. (총 29점)

- 1) H-IDS와 N-IDS의 동작 특성을 설명하시오. (8점)
- 2) 아래는 오픈소스 기반 IDS인 스노트(Snort)의 어떤 규칙이다. 이 규칙의 의미를 각 줄별로 구체적으로 설명하시오. (21점)

①	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 4000 \
②	(msg: "login buffer overflow attempt"; \
③	flow: established, to_server; \
④	content: "username="; depth: 16; offset: 4; nocase; \
⑤	content: "passwd="; within: 20; distance: 4; nocase; \
⑥	isdataat: 400, relative; \
⑦	content: ! " 0A "; within: 400; \
⑧	classtype: attempted-admin;)

인사혁신처 시험출제과장