3 교 시	시스템네트워크보안	사 이 버

※ 답안지에 수정액, 수정테이프 사용은 불가하며, 오류기재 시 옆으로 두줄금을 그어 다시 기재하시기 바랍니다.

【문 1】 다음은 버퍼 오버플로우 공격 기법(Buffer Overflow Attack)에 대한 문항이다. 아래 물음에 답하시오. (50점)

(1) 힙(Heap) 버퍼 오버플로우와 스택(Stack) 버퍼 오버플로우 기법에 대해 기술하시오. (20점)

(2) 다음은 버퍼 오버플로우를 일으킬 수 있는 취약한 C언어 함수이다. 해당 함수를 보완한 안전한 함수의 이름과 안전한 이유에 대해 기술하시오. (15점)

```
strcpy(char *dst, const char *src)
```

(3) 다음의 스택 버퍼 오버플로우 대응 기술에 대해 기술하시오. (15점)

① 스택 가드(Stack Guard)

② 스택 쉴드(Stack Shield)

③ 주소 공간의 임의 추출(ASLR)

【문 2】 포트 스캐닝(Port Scanning)은 어떤 포트가 열려 있는지 확인하는 것으로 침입 전 취약점을 분석하기 위한 사전 작업 중 하나이다. 아래 물음에 답하시오. (20점)

(1) TCP Connect(Open) 스캔에 대해 약술하시오. (6점)

(2) TCP FIN · NULL · Xmas 스캔을 각각 설명하고, SYN 스캔(Half-Open Scan)과의 응답 결과에 대한 차이점을 약술하시오. (8점)

(3) Decoy 스캔에 대해 약술하시오. (6점)

【문 3】 스위치 환경에서 가능한 스니핑 공격 기법에 대해 약술하시오. (30점)