네트워크 보안 점검(침투시험) 범위 설정:

1. **귀사의 가장 큰 보안 위험은 무엇입니까:**
(예: 웹사이트 변조, 고객 정보 해킹, 내부자 정보 유출, 시스템/네트워크 DDoS 공격 등을 포함해서 작성)

가장 큰 보안 위험은 고객 민감정보(개인정보 또는 신용카드 정보)가 제대로 보호되고 있는 지이다.

2. 구체적 점검 대상 컴퓨터/서버 주소 범위, 애플리케이션

프라이머리 DMZ: 서버 20대 및 IP 주소 40개: _____

세컨더리 DMZ: 서버 25대 및 IP 주소 50개: _____

3. 점검 대상에서 제외할 서버/컴퓨터, 네트워크 장비/주소 또는 애플리케이션은:

DNS 서버 1대 : _____

방화벽 2대: _____

라우터 2대:_____

4. 2번 점검 대상 서버 중에 외부기관에서 소유한 것이 있으면 나열:

5. 점검 시험 시간은(예: 업무시간, 업무외 시간, 주말 등):_____

6. 점검은 실제 시스템으로 대상인지 아니면 시험용 서버 환경인지:

_____

7. 점검은 아래의 기법을 포함해도 되는 지:

네트워크에 Ping sweep: _____

점검 대상 서버에 포트 스캔: _____

점검 대상 서버에 (로컬/원격)취약점 스캔: _____

점검 대상 서버 해킹: _____

애플리케이션 공격: _____

클라이언트 측 공격(자바/액티브X)등 역공학: _____

물리적 침투 시도: _____

직원 대상 소셜 엔지니어링: _____

기타: _____

8. 점검은 내부 네트워크를 대상으로 해도 되는가(예/아니오): _____

그렇다면 내부 네트워크에는 어떻게 접근할 수 있는지(예: 내부에서 시험, 외부에서 침투, 무선 AP로 접근 등): _____

_____

9. 클라이언트/사용 PC도 점검 범위에 포함하는 지(예/아니오): _____

10. 소셜 엔지니어링 기법도 가능한지:_____

11. DoS 공격도 가능한지(예/아니오): _____

12. 위험한 점검/익스플로잇도 가능한지(예/아니오): _____

ITL시큐어인스티튜트

주소: 경기도 성남시 분당구 백현로 97번지,
다운타운빌딩 1207호

전화번호: 031)717-1447

대표: (인)

서명일: 년 월 일

고객사:

주소:

전화번호:

성명: (인)

서명일: 년 월 일