해킹 및 침해대응 중간고사 (담당:이재광)

학번 :　　이름 :

1. 아래 그림(3강 기업의 보안체계, 5page)은 일반적인 기업의 네트워크 환경을 나타내고 있다. 그림을 참고하여, 침해대응 관점에서 기업이 수행해야 하는 정보보호 노력에 대해 논리적으로 서술하시오.

   (단, 아래 작성 가이드에 제시된 항목을 반드시 포함시켜야 함)

[작성 가이드]

(1) 기업 환경에 존재하는 다양한 Attack Surface 제시

(2) 네트워크 구성 측면에서 DMZ 서버 영역이 가지는 특징 제시

- 그 특징으로 인해 발생되는 Risk 설명
- 해당 Risk와 관련하여 필요한 정보보호 노력 설명

(3) 네트워크 구성 측면에서 사용자 영역이 가지는 특징 제시

- 그 특징으로 인해 해커가 사용하는 해킹 기법 설명
- 해당 해킹 기법과 관련하여 필요한 정보보호 노력 설명

(4) 해커가 업무 서버 영역을 공격하기 위해 수행할 수 있는 공격 방식 제시

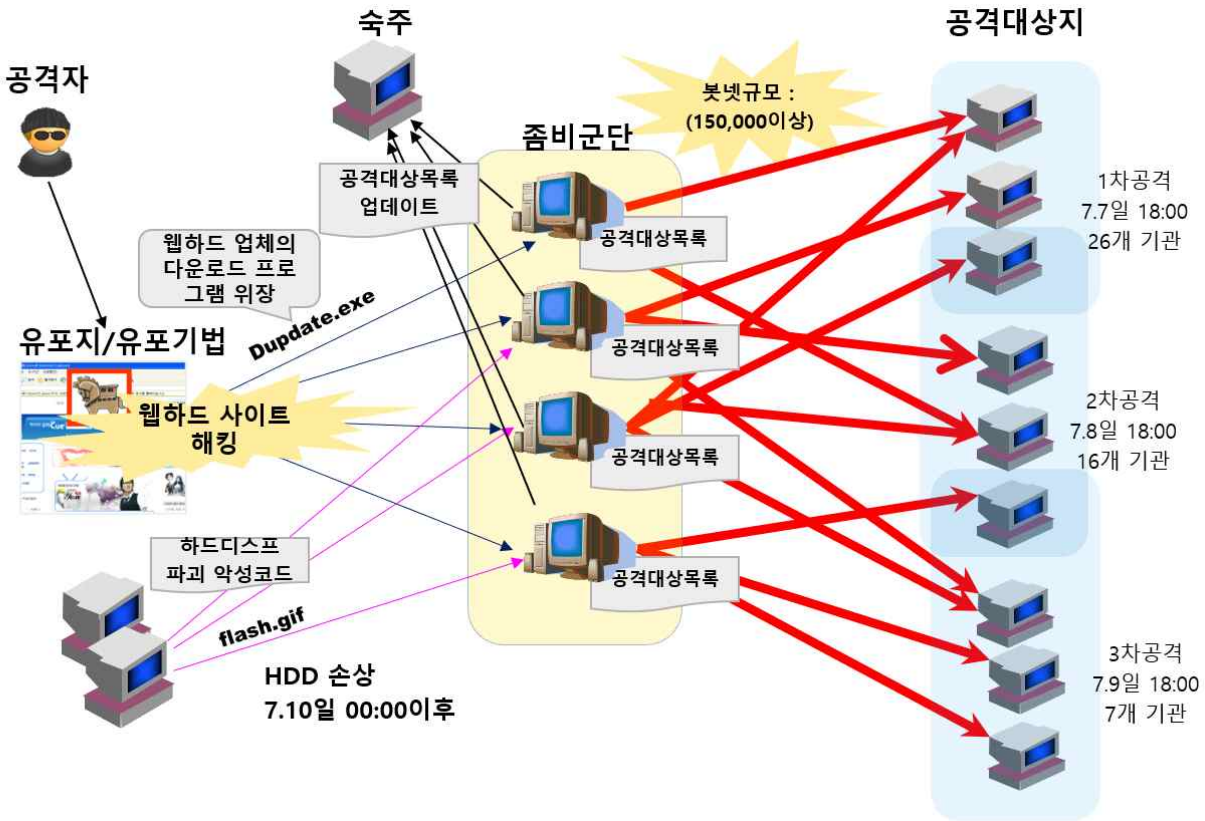
- 해당 공격 방식을 대응하기 위해 필요한 정보보호 노력 설명

(5) 고도화되어가는 사이버공격 대응을 위해 보안관제(분석) 영역에서 수행해야 하는 정보보호 노력(또는 방향성) 제시

이곳에 답안을 작성하세요. (분량 제한 없음)

2. 아래 그림(4강 디도스 공격과 봇넷대응, 5page)은 2009년 7월 7일 발생된 디도스 공격의 사고 개요도이다. 해당 사고 대응 및 예방을 위해 KrCERT/CC에서 수행해야 하는 역할(or 대응과정)에 대해 상세히 설명하시오.

(단, 아래 작성 가이드에 제시된 항목을 반드시 포함시켜야 함)



[작성 가이드]

(1) 공격 발생 인지 후부터 진행되는 전체 대응과정의 우선순위 제시

(2) 유관 기관(통신사, 백신사 등)과의 협력이 필요한 영역과 방법, 필요성 제시

(3) 좀비PC가 특정 기업 內 존재하는 직원 PC로 확인될 경우, KrCERT/CC에서 해당 기업의 정보보호 담당자에게 가이드 해 주어야 하는 내용 제시

(4) 'DNS 싱크홀'과 '허니넷'이 디도스 대응 관점에서 갖는 차이(역할, 활용성 등) 제시

이곳에 답안을 작성하세요. (분량 제한 없음)

학번 및 이름을 쓰셨는지 확인해주세요. 수고 많으셨습니다.