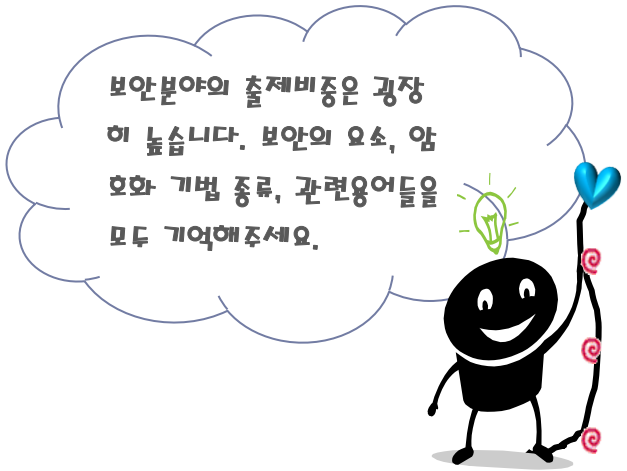
제 4과목 – 신기술 동향 및 시스템 관리

I. 정보보안 및 관련용어 정리



오늘의 핵심내용

- 정보보안 요소 및 위협형태
- 암호화 기법 및 프로토콜 학습
- 보안관련 용어 학습

✓정보 보안의 개념

- 시스템 내에 있는 프로그램과 데이터에 대해 통제된 접근 방식을 다루는 것을 의미
- 네트워크에 연결된 컴퓨터 시스템의 정보나 데이터를 공개, 변조, 파괴 등으로부터 보호하는 것

정보 보안의 요소

속성	설명
기밀성(비밀성, confidentiality)	정보를 인가된 시간, 사용자, 기관에게만 공개 또는 처리하는 것으로 공개로부터 정보를 보호.
무결성(완전성, integrity)	데이터를 정확하고 완전한 상태로 보존하는 것으로 외부로부터 정보를 변조하려는 시도로부터 보호.(인증받은 사용자만 데이터를 수정할 수 있도록 하고, 전달과정에서 데이터 훼손되지 않도록 보호)
인증성(authentication)	정보를 보내는 사람의 신원을 확인 네트워크에 접속하는 사용자 계정 등을 확인하여 거짓 인증으로부터 시스템과 정보를 보호
가용성(availability)	사용권한이 부여된 사용자는 언제든지 시스템을 사용할 수 있도록 하는 것
접근제어(access control)	정보를 인가된 사용자에게만 접근하도록 제어 시스템의 자원 이용에 대한 불법적인 접근을 방지 데이터 보호나 비밀 유지 등으로 컴퓨터의 접근 통로를 최소화
부인방지(non-repudiation)	송신자의 송신 여부와 수신자의 수신 여부를 확인 정보 제공자 또는 수신자가 상대방의 정보 내용에 대해 부인하는 것을 방지

✓ 암호화기법

- 데이터에 암호 알고리즘을 적용하여 허가 받지 않은 사람들이 정보를 쉽게 이해할 수 없도록 데이터를 암호문이라고 불리는 형태로 변환하는 기법을 의미

비밀키 암호화 기법

- DES(Data Encryption Standard) 알고리즘 사용하며, 동일한 키로 데이터를 암호화하고 복호화
- 복호화 키를 아는 사람은 누구든지 암호문을 복호화 할 수 있어 복호화 키의 비밀성을 유지하는 것이 중요!
- 암호화/복호화의 속도가 빠르며, 알고리즘이 단순하고 파일 크기가 작음
- 사용자의 증가에 따라 관리해야 할 키의 수가 상대적으로 많아지는 것이 단점
- 대칭 암호화 기법, 단일키 암호화 기법이라고도 함

공개키 암호화 기법

- RSA(Rivest Shamir Adleman) 알고리즘 사용
- 서로 다른 키로 데이터를 암호화하고 복호화 수행
- 데이터를 암호화할 때 사용되는 키(공개키)는 공개하고, 복호화할 때의 키(비밀키)는 비밀로 함.
- 키의 분배가 용이하고 관리해야 할 키의 개수가 적다.
- 암호화/복호화의 속도가 느리며, 알고리즘이 복잡하고 파일 크기가 큼
- 비대칭 암호화 기법

✓ 암호화 프로토콜

1. SSH(Secure Shell)

• 가장 많이 쓰이는 암호화 프로토콜
• 네트웍상의 다른 컴퓨터에 인증을 통한 로그인과 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 함
•telnet, ftp 를 암호화하여 전송
•스니핑 공격을 막고, 기존의 rsh, rlogin, rcp 등을 대체하기 위해 설계되었으며, 강력한 인증방법 및 안전하지 못한 네트워크에서 안전하게 통신을 할 수 있는 기능을 제공

2. 전자서명(digital signature)

• 자료를 송신한 사람이 추후에 부인할 수 없도록 신원을 증명하기 위한 서명
•특정인을 확인하기 위해 공개키 암호방식(RSA)을 사용
•메시지를 받는 사람이 메시지를 위변조 할 수 없으며, 재사용이 불가능
•송수신자 신분을 암호화된 데이터로 메시지에 덧붙여 보내기도 하며, 전자상거래를 활용할 수 있음

3. 커베로스(Kerberos)

• 개방된 네트워크에서 서비스 요구를 인증하기 위한 방법으로 미국 MIT Athena 프로젝트에서 개발

•분산 컴퓨팅 환경에서 대칭키를 이용하여 사용자 인증을 제공하는 중앙 집중형 인증(authentication) 방식

•사용자가 서버의 인증을 얻기 위해서 티켓 이라는 인증 값을 사용

•개체

- ➢클라이언트 : 인증을 얻길 원하는 사용자의 컴퓨터
- ➢서버 : 클라이언트가 접속 하려고 하는 컴퓨터
- ➢인증 서버 : 클라이언트를 인증 하는 컴퓨터
- ➢티켓 발급 서버 : 인증 값인 티켓을 클라이언트에게 발급 해 주는 컴퓨터

•개방된 다른 기종간의 컴퓨터에서 자유로운 서비스 인증(SSO)이 가능

•대칭키를 이용하면 도청으로부터 보호받을 수 있지만 패스워드 사전 공격에는 취약

•타임스탬프(Time stamp)로 클라이언트와 서버에 시간 동기화 프로토콜이 필요하고, 재생 방지 공격을 위해 유효기간을 표기해야 함

✓ PKI(Public Key Infrastructure 공개키 기반 구조)

•공개키 인증서의 인증성(무결성)을 제공하기 위한 신뢰구조
•안전한 PKI는 인터넷 전자상거래 시스템뿐만 아니라 범국가적 정보통신망에서도 중요한 역할 수행
•사용자 공개키와 사용자 ID를 안전하게 전달하는 방법과 공개키를 신뢰성 있게 관리하기위한 수단 제공
•인증서 발급, 인증서 사용/취소 관련 서비스를 통해 기밀성, 무결성, 접근제어, 인증, 부인방지의 서비스제공

✓보안위협

보안을 위협하는 요소

도청(wiretapping)	전송중인 자료나 정보를 몰래 빼내는 행위
스니핑(snifing)	•호스트에 전송되는 정보(아이디,패스워드)등을 엿보는 행위 •패킷 내용을 중간에서 도청하므로 암호화 프로토콜을 이용하여 통신
스푸핑(spoofing)	•"속임수"의 의미로 어떤 프로그램이 정상적으로 실행되는 것처럼 위장하는 행위 •신뢰성 있는 사람이 네트워크를 통해 데이터를 보낸 것처럼 허가받지 않은 사용자가 데이터를 변조하여 접속하는 행위 •무관한 ip주소를 마치 접근 가능한 클라이언트 ip인 것처럼 위장하여 침입
트랩도어 (trap door)	•응용 프로그램이나 운영 체제 개발시 프로그램 오류를 쉽게 발견하기 위해 코드 중간에 중단부분을 만들어 놓는 행위 •트랩도어를 삭제하지 않고 다른 용도로 악용
백도어 (back door)	•시스템에 무단 접근하기 위해 사용되는 일종의 비상구로 컴퓨터의 보안 예방책에 침입하는 행위 •시스템 장애 대비하여 제작회사에서 해당 시스템에 직접 접속하여 점검할 수 있도록 개방한 특정 계정 의미
트로이목마	•어떤 허가되지 않은 행위를 수행시키위해 시스템에 다른 프로그램 코드로 위장 침투하는 행위 •평상시에는 정상적 프로그램으로 유지되다가 특정 프로그램이 실행되면 시스템에 손상을 주는 프로그램

서비스 거부 공격 DoS	•일시에 대량의 데이터를 한 서버에 집중 전송시켜 특정 서버를 마비시키는 행위 •접속 트래픽과 DoS공격 패킷을 구분하기위해 모니터링 툴과 침입방지 시스템을 이용
분산 서비스 거부 공격 DDoS	•해킹 프로그램을 이용하여 여러 사용자의 컴퓨터가 특정 사이트에 고용량의 패킷을 연속적으로 보내도록 하여 해당 사이트의 시스템을 마비시키는 방식 •송신측의 IP를 속이리 수 있으며, 피해 시스템 운영이 불가능

데이터 보안 침해 형태

가로막기 (Interruption)	데이터 전달을 가로막아 수신측에 정보가 전달되는 것을 방해하여 정보의 가용성을 저해
가로채기 (interception)	전송되는 데이터를 도청 및 몰래 가로채기하여 정보의 기밀성을 떨어뜨림
변조/수정	원래의 데이터가 아닌 다른 내용으로 수정하여 변조시키는 것으로 정보의 무결성을 떨어뜨림
위조 (fabrication)	사용자 인증과 관계되어 다른 송신자로부터 데이터가 온 것처럼 꾸미는 것으로 정보의 인증성을 떨어뜨림

1.패킷 스니핑(snipping)

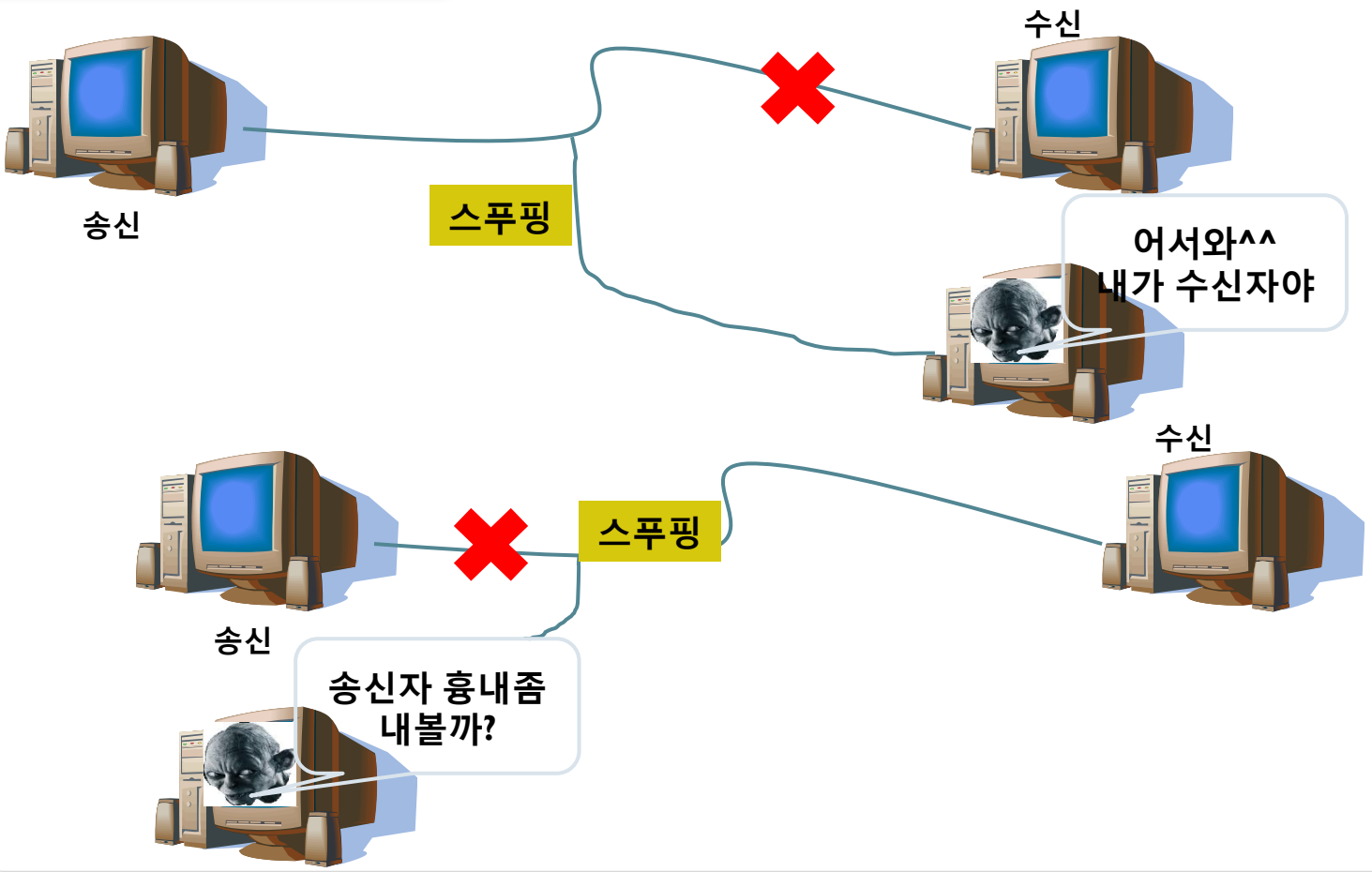
•네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는(도청)행위를 의미

•Tcp/ip 프로토콜을 이용한 통신에서는 통신매체를 통과하는 패킷들이 암호화가 되어있지 않은 상태이므로 이 패킷을 도청하여 메시지 내용을 볼 수 있음

- 모니터링 포트 (미러링 포트) - 스위치를 통과하는 모든 트래픽을 볼 수 있는 모니터링 포트가 있고 여기서 네트워크 사용량, 응답시간등과 같은 장비 성능을 관리 ,공격자가 여기에 자신의 PC를 연결하면 스니핑이 가능

- 스위치 재밍(Jamming) – 스위치가 ip주소를 MAC주소로 변경하기위해 내부적으로 관리하는 매핑 테이블의 최대 저장개수보다 더 많은 정보를 추가하여(오버플로우)스위치가 브로드캐스팅 모드로 전환하도록 하는 것=➔ 자신이 전달받은 모든 패킷을 연결된 다른 pc에 전달하는 모드가 됨을 의미

2. 스푸핑(spooping)



- 마치 자신이 수신자인 것처럼 행세하여 송신자가 보낸 메시지를 강탈
- 송신자로 행세하는 스푸핑은 서비스 거부 공격(Dos)의 수단이 되기도 함.

3.세션 하이제킹(session hijacking)

- 상대방 세션을 가로채는 지능적 공격기법
- 정당한 접근권한을 획득한 사용자가 패스워드를 성공적으로 입력하여 로그온 후에 공격자는 현재의 연결된 세션을 넘겨받아 그 사용자처럼 위장
- 공격자는 서버로의 접근을 위해 id,패스워드를 사용하는 인증절차를 건너뛸 수 있음

웹 보안

종류	특징
SSL	•웹 브라우저와 서버를 위한 보안 방법으로 비대칭형 암호 시스템을 사용 •데이터 송수신하는 두 시스템 사이 즉, tcp/ip 계층과 응용계층 사이에 위치하여 인증, 암호화, 무결성을 보장하는 표준 프로토콜
SET	•신용카드나 금융 거래 안전을 위한 보안 접근 방법제시 •메시지 암호화, 디지털 서명 기능
SEA	•전자서명, 암호 등을 통해 보안을 구현 •SSL,S-HTTP 의 단점을 보완
S-HTTP	•웹에서 안전하게 파일 교환을 할 수 있는 HTTP의 확장판(전자서명 지원)

방화벽

- **보안이 필요한 네트워크의 통로를 단일화하여 관리함으로써 외부의 불법 침입으로부터 내부의 정보 자산을 보호하기 위한 시스템**

•내부로 들어오는 패킷은 인증된 패킷만 통과시키는 구조

•역추적 기능이 있어 외부의 침입자를 역추적하여 흔적을 찾을 수 있음

•내부로부터 불법적인 해킹은 막지 못함

프록시 서버 – 인터넷을 사용하는 기관에서 사용자와 인터넷 사이의 중개자 역할 담당하는 서버로 방화벽 시스템 내에 있는 사용자들이 방화벽 외부에 있는 서버에 서비스의 요구와 응답을 자유롭게 할 수 있도록 하는 시스템을 의미

→ 방화벽 기능과 캐쉬 기능 두 가지 모두를 동시에 제공해 준다.

→ 방화벽 기능 – 방화벽 설치하는 경우 외부와 통신연결이 가능하도록 HTTP, Gopher, FTP 프로토콜 지원

◆ 침입 탐지 시스템(IDS)

악의적인 시스템 강제 조작을 탐지하는 역할을 하는데 방화벽이 탐지할 수 없는 종류의 네트워크 트래픽 및 컴퓨터 사용을 탐지하는 시스템을 의미

•장점

① 해킹방법을 기반으로 해커의 침입을 탐지하므로 신기술의 적용이 빠름
② 외부로부터의 공격 뿐만 아니라 내부자에 의한 해킹도 차단가능
③ 접속하는 ip에 상관없이 침입을 차단
④ 시스템 침입에 즉시 대응
⑤ 해킹사실 발견시 해킹에 관한 정보를 휴대전화, 무선호출기, e-mail등으로 즉시 전송

◆ 침입 방지 시스템(IPS-Intrusion Prevention System)

▪여러가지 보안기술을 이용하여 공격자가 침입하는 것을 방지

▪일종의 경보시스템으로 인증, 방화벽, 바이러스 등 유해 트래픽을 차단하기위한 능동형 보안 솔루션

▪침입탐지 시스템과 달리 침입을 탐지했을 경우에 대한 대처까지 수행

◆ VPN(가상사설망,Virtual Private Network)

➢기존 사설망의 고비용과 비효율적 관리를 해결하기위한 방법으로 인터넷 망을 마치 전용선처럼 사용할 수 있는 네트워크로써 기업의 통신망과 인터넷 서비스 제공자와의 연결만 하면 되므로 기존의 사설망 연결방식보다 비용절감효과가 있다. 단, 정보에 대한 보안이 미약하다.

◆ IPSec 프로토콜

- IP망에서 안전하게 정보를 전송하는 표준화된 3계층 터널링 프로토콜
- 인터넷 상에서 전용회선과 같이 이용 가능한 가상 전용회선을 구축하여 데이터가 도청당하는 위협으로부터 방지를 위한 통신 프로토콜

◆ 데이터 유출방지(DLP,Data Leakage Preventing)

- 내부 직원이 사용하는 pc와 네트워크상의 모든 정보를 검색하고 사용자의 행위를 탐지/통제해 외부로의 정보유출을 사전에 방지한다.

◆ PET(프라이버시 강화기술, Privacy Enhancing Technology)

- 개인정보 침해위험을 관리하기 위한 핵심기술로 암호화, 익명화 등 개인정보를 보호하는 기술

◆ 디지털 포렌식(Digital Forensics)

- 컴퓨터, 휴대전화,인터넷 등의 디지털 저장매체에 존재하는 디지털 정보를 수집하는 디지털 수사과정 의미

◆ WPA(Wi-Fi Protected Access)

➢wi-fi에서 제정한 무선랜 인증 및 암호화 관련 프로토콜의미. 암호화는 웹 방식을 보완한 IEEE802.11i 표준의 임시 키 무결성 프로토콜을 기반으로 하며, 인증 부문에서도 802.1x 및 확장 가능 인증 프로토콜을 기반으로 상호 인증 도입하여 성능을 높임.

◆ i-pin(인터넷 개인식별번호,internet Personal Identification Number)

➢주민번호 대신 인터넷상에서 사용할 수 있도록 만든 사이버 주민번호를 의미. i-pin은 사용자에 대한 신원확인절차가 완료되면 본인확인기관에 의해 온라인으로 사용자에게 발행된다.

◆ CAPTCHA(자동 계정 생성 방지 기술, Completely Automated Public Turing test to tell Computers and Humans Apart)

- 사용자도 모르게 악의적으로 웹페이지에 회원가입을 하거나 스팸메시지를 보내기 위해 사용하는 봇(bot)을 차단하기 위해 만들어짐.

◆ 봇넷(Botnet)

- 악성 프로그램에 감염되어 향후에 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 의미한다. 해킹 또는 악성 프로그램에 감염된 컴퓨터를 네트워크로 연결하고, 해커는 봇넷에 연결된 컴퓨터를 원격조종해 개인정보유출, 스팸메일 발송, 다른 시스템에 대한 공격 등 악의적인 행위를 함.

◆ 파밍(pharming)

➢합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 DNS 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도하여 개인정보를 훔치는 인터넷 사기수법

◆ Typosquatting

➢특정 사이트 접속시 주소를 잘못 입력하는 경우 이와 유사한 유명 도메인을 미리 등록하는 것으로 'URL 하이재킹'이라고도 함

◆ Ransomware(랜섬웨어)

- 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 파일 등을 임의로 암호화해 사용자가 알지 못하도록 만든 후 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 하는 신종 악성 프로그램

◆ VoIP 보안 위협(VoIP Security Threat)

- 음성 패킷을 불법으로 수집 및 조합해 통화 내용을 재생하고 도청(sniffing)하는 위협이다.
- 서비스 관련 시스템 자원 고갈 및 비정상 패킷의 다량 발송을 통한 회선 마비 등의 서비스거부(dos)공격이 있다.

◆ Zero day attack(제로 데이 공격)

- 보안의 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이뤄지는 공격기법으로 취약점에 대한 대응책이 마련되기 전에 공격이 이뤄지므로 대처 방법이 없다.

이장의 핵심 콕!콕! 기출 따라잡기

1. 아래 지문은 어떤 보안관리와 관련된 설명이다. 해당하는 관리기법을 영문약자로 쓰시오.

데이터의 안전한 배포를 활성화하거나 불법 배포를 방지하여 인터넷이나 기타 디지털 매체를 통해 유통되는 데이터의 저작권을 보호하기 위한 시스템이다. 이 시스템은 디지털워터마크의 사용 또는 이와 유사한 방식으로 콘텐츠를 작성하여 콘텐츠가 제한 없이 보급되지 않도록 하거나 데이터를 암호화하여 인증된 사용자만이 접속할 수 있게 하여 지적재산권을 보호한다..

답 : _____

2. 아래 지문에서 설명하는 용어를 영문 약자로 쓰시오.

최근 심각한 위험으로 대두되고 있는 개인정보 침해위협을 관리하기 위한 핵심기술로 암호화, 익명화 등 개인정보를 보호하는 기술에서 사용자가 직접 개인정보를 통제하기 위한 기술까지 다양한 사용자 프라이버시 보호 기술을 통칭한다.

답 : _____

3. 아래 지문의 빈 칸에 들어갈 용어를 영문약어로 쓰시오.

( )는 서비스 기술자나 유지 보수 프로그램 작성자의 엑세스 편의를 위해 시스템 설계자가 고의로 만들어놓은 시스템 보안이 제거된 비밀통로이다. 대규모의 응용프로그램이나 운영체제(os)를 개발할 때는 프로그램 보수의 용이성을 위해 코드 중간 중간에 ( )라는 중단 부분을 설정하는데, 최종 단계에서 이 부분을 삭제하지 않고 남겨두면 컴퓨터 범죄에 악용되기도 한다.

답 : _____

4. 아래 지문에서 설명하는 보안 위협 용어를 영문으로 쓰시오.

표적으로 삼은 특정 집단이 주로 방문하는 웹 사이트에 악성 코드를 심어놓고, 표적 집단이 그 웹 사이트를 방문할 때까지 기다리는 웹 기반 공격이다. 공격자는 사전에 표적 집단이 자주 방문하는 웹 사이트를 조사하고 그 웹 사이트에 악성 코드를 심어 놓는다. 악성 코드에 감염된 웹 사이트의 방문자는 모두 악성코드에 감염되므로 전염성이 높다.

답 : _____

5. 아래 괄호() 안에 공통적으로 들어갈 용어를 쓰시오.

( )은 사람들이 여러 웹페이지에 로그인하거나 결제 정보를 입력하는 등 온라인 활동을 하면서 남긴 기록으로, 구매 패턴, 속성, 결제방법,구매 이력 내용, SNS, 전자우편(e-mail), 홈 페이지 방문 기록, 검색어 기록 등이 이에 해당된다.
( )을 바탕으로 기업은 고객 맞춤형 디지털 광고나 판촉 활동을 벌일 수 있지만 최근 이를 통한 개인 정보 유출에 대한 피해 사례가 많아지면서 이런 기록들을 제거해주는 전문업체도 생겨났다.

답 : _____

정답

1. 답 - DRM

2. 답 - PET

3. 답 – back door , trap door

4. 답 - watering hole

5. 답 – digital footprint