5차시. 4차 산업혁명의 안전띠 '사이버보안' 이해

01. 5G 사이버 보안의 이해

- 4차 산업혁명 시대가 도래 하면서 사이버 보안에 집중해야 하는 분명한 이유는 초 연결 기반의 사이버공간이 중요해지기 때문이다. 4차 산업 혁명 시대를 견인하는 초 연결 기반이라는 것은 사이버공간과 현실공간이 서로 연결된 사이버 물리 시스템이기 때문에 네트워크 기반의 사이버 공격으로 사회적 인프라에 피해를 유발할 수 있고 그 피해규모가 과거와는 다르게 대형화 되어 사이버 보안에 집중해 피해규모를 줄여야 한다. 아울러 사이버 공격이 더 쉬워졌다. 이것은 4차 산업혁명으로 인한 기술 발전은 전문적인 해커는 물론 누구나 손쉽게 사이버공격이 용이해져 네트워크를 통한 사이버 공격이 일상화 되면서 사회적 혼란이 지속될 수 있음을 의미한다.
- 이번 차시에서는 4차 산업혁명의 안전띠 역할을 하는 사이버 보안에 대한 기본적이고 개괄적인 내용을 학습한다. 즉, 사이버 보안 관련 용어 정리에서부터 사이버 보안 목표, 사이버 보안 구조를 학습하고 이어서 일반적인 해킹 프로세스를 학습하여 사이버 보안에 대한 대응력을 높이도록 한다.

사이버 보안 개념

- **사이버 보안의 목표**

  미국 상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소인 미국표준기술연구소(NIST: National Institute of Standards and Technology)의 컴퓨터 보안 핸드북에 따르면 컴퓨터 보안은 다음과 같이 정의된다.

> NIST Definition: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"

즉, "컴퓨터 시스템의 자원(H/W. S/W, F/W, 정보/데이터, 통신)에 대한 무결성, 가용성, 기밀성 달성을 위한 자동화된 정보 시스템에 제공된 보호"로 표현된다. 이 정의에 의하면 컴퓨터 보안에 있어서 가장 핵심적인 개념인 소위 말해서 CIA(Confidentiality, Integrity, Availability의 각 첫 알파벳) 트라이어드(triad)라고 한다. 이 세 가지 개념은 데이터에 대한 정보보호와 함께 정보 서비스에 관한 기본 보안 목적을 구체적으로 설명하고 있는 것이다.

사이버 보안의 목표

- 기밀성(Confidentiality): 개인정보나 기밀정보를 부정한 사용자가 이용하거나 그들에게 노출되지 않도록 하는 것으로 정보접근과 공개에 대해 합법적인 제한조건을 준수하는 것이다. 여기에는 개인 프라이버시와 정보를 보호하는 수단을 포함하며 기밀성을 상실하게 되면 정보가 부정하게 공개된다. 기밀성에는 두 가지 의미가 있다.

. 데이터 기밀성: 개인 정보나 기밀정보를 비 인가자에게 노출 되지 않도록 함

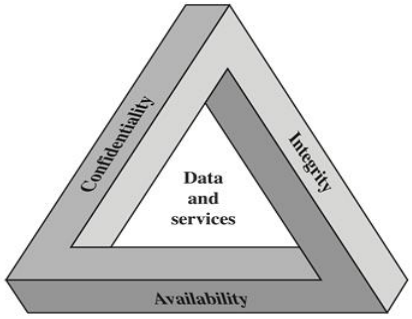
. 프라이버시(Privacy): 개인 관련 어떤 정보가 수집되고 저장되는지, 누구에게 공개되는지, 누가 공개하는지 등을 통제하거나 영향을 미칠 수 있도록 하는 것

- 무결성(Integrity): 부적절한 정보 수정이나 정보 파괴를 차단하는 것이다. 정보 부인 방지와 합법성을 명확히 하는 수단이 포함되며, 무결성을 상실하게 되면 정보가 무단 수정되거나 파괴될 수 있다. 무결성에는 두 가지 의미가 있다.

. 데이터 무결성: 인가 상태에서만 정보나 프로그램을 변경할 수 있도록 보장하는 것

. 시스템 무결성: 시스템이 의도했던 기능으로 동작하고 비인가자에 의해서 시스템이 조작되지 않은 상태로 수행하도록 보장하는 것

- 가용성(Availability): 시스템이 지체 없이 동작하도록 하고, 합법적인 사용자에게 서비스를 거절하지 않도록 하는 것으로 정보사용에 있어서 시간성과 신뢰성 있는 접근을 보장하는 과정이다. 가용성이 상실되면 정보나 정보 시스템 사용과 접근이 불가능하다.



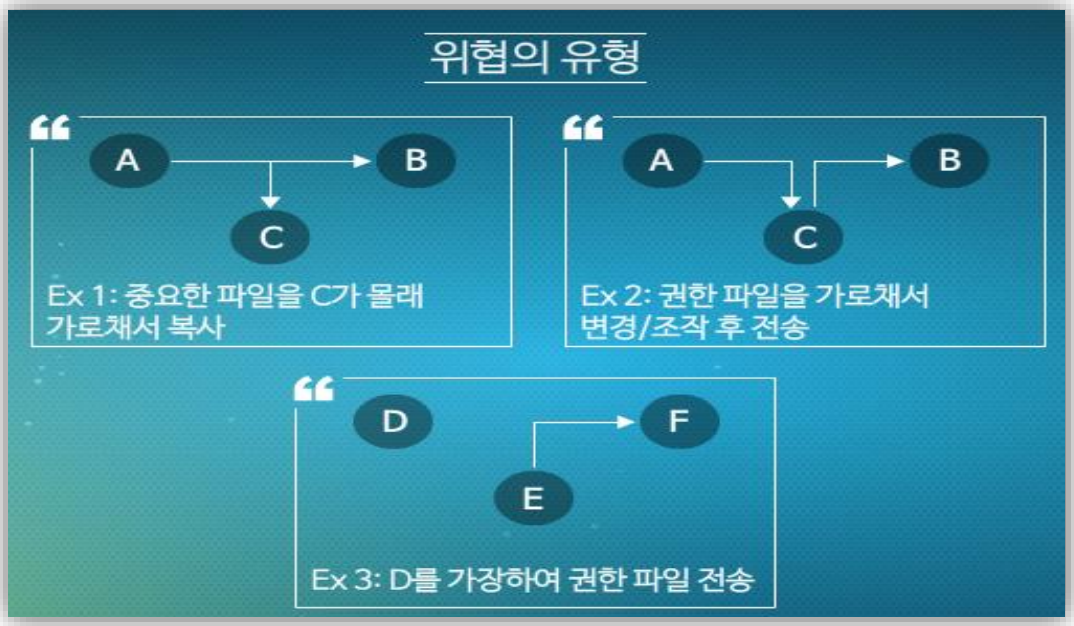
CIA 트라이어드를 통해서 보안의 목표를 잘 정의했지만 추가적으로 인증(Authenticity)과 책임성(Accountability)을 추가하여 보안 목적을 완성되게 표현한다.

- 인증: 사용자가 진짜 인가된 사용자인지, 시스템에 도착한 자료가 정말 신뢰할 수 있는 출처에서 온 것인지에 대한 확신을 제공하는 것이다.
- 책임성: 개체의 행동을 유일하게 추적해서 찾아낼 수 있어야 한다는 사항이 포함되어야 한다. 여기에는 부인봉쇄, 책임성 추적, 포렌식 등이 포함된다.

사이버 위협의 정의(RFC 4949)

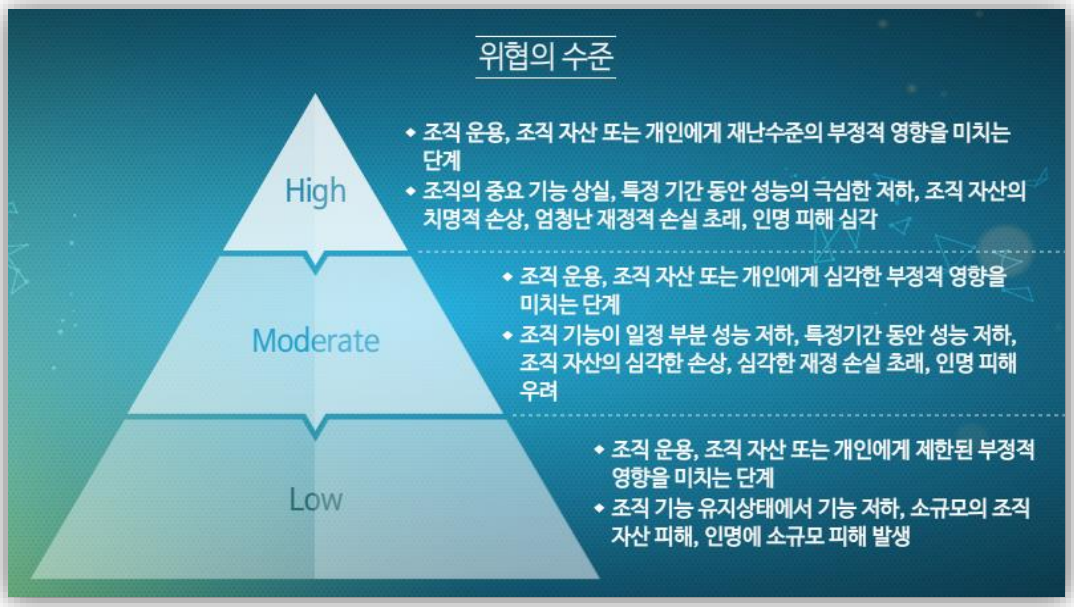
사이버 보안에 대한 본격적인 이해에 앞서 사이버 보안 관련 중요 용어인 사이버 위협에 대하여 인터넷 표준인 RFC 4949에 정의한 내용을 알아본다.

- 위협이란 보안 취약점을 악용하려는 잠재적인 위험으로 보안 침해와 손상을 유발하는 환경, 능력, 행동, 사건을 의미한다.



- **사이버 위협의 정의(RFC 4949)**

  – 위협 수준은 아래의 그림에서와 같이 재정적 손실이나 인명 피해, 개인이나 조직에 미치는 영향 등을 기준으로 상, 중, 하로 구분하며 위협에 따른 사이버 공격에 대한 경보 발령 시에 기준으로 사용하기도 한다.



사이버 보안 구조(Security Architecture)

- ITU-T 권고안 X.800의 OSI(Open System Interconnection) 보안 구조에서는 보안 관리자가 효과적으로 보안문제를 조직화할 수 있는 유용한 방법을 제공하고 있다. 보안 구조의 핵심으로 보안 공격, 보안 메커니즘 그리고 보안 서비스를 정의하고 있다. 이 보안 구조는 국제적으로 표준화되어 있기 때문에 관련 기업에서는 보안구조에서 권고된 서비스와 메카니즘에 대한 정의를 그들의 제품과 서비스에 반영하기 때문에 사이버 보안을 이해하는데 매우 유용하다.

  - 보안공격(security attack) : 조직 소유의 정보보호를 손상하는 모든 행위

  - 보안 매커니즘(security mechanism)

  . 보안 공격으로부터 탐지, 차단 또는 복구를 위해 설계된 프로세스

  . 보안 프로세스를 수행하는 디바이스 - 보안 서비스(security service)

  . 조직에서 데이터처리 시스템과 정보 전달에 대한 보안성을 강화하는 프로세스 또는

  . 보안 공격에 대응하는 목적으로 서비스를 제공하기 위하여 하나 이상의 보안 메커니즘을 이용하여 서비스 제공

- **보안 공격(Security Attacks)**

  보안 공격의 개념은 조직 소유의 정보보호를 손상하는 모든 행위를 포함하며 보안 공격은 소극적 공격(passive attack)과 적극적 공격(active attack)으로 분류한다.

  소극적 공격은 시스템에서 정보를 취득만 할뿐 시스템 자원에는 영향을 주지 않는다(아래 그림 참고). 즉 트래픽을 모니터링하거나 도청이 목적이다. 소극적 공격의 목적은 메시지 내용을 공개 한다거나 트래픽을 분석하여 그것을 바탕으로 후속 공격에 활용하는 것이다.

보안 공격(Security Attacks)

적극적 공격은 시스템 자원을 변경하거나 운용에 영향을 미치는 공격을 말한다(아래그림 참조). 즉, 전송 데이터를 변조하거나 허위 정보를 생성하는데 물리적, 소프트웨어 및 네트워크의 다양한 취약점이 존재하기 때문에 차단이 어렵다. 그 대응으로는 공격 탐지, 피해 복구, 피해 확산 지연을 위한 수단이 필요하다.

적극적 공격 유형으로는 신분위장, 재전송, 메시지 변조 그리고 서비스 거부가 있다.

- 신분 위장((Masquerade): 한 개체가 다른 개체 행세를 하는 것으로 다른 유형의 공격과 병행해서 발생. 예를 들어 인증 메시지 갈취 후 신분위장
- 재전송(Replay): 소극 공격으로 획득한 정보를 보관하였다가, 시간 경과 후 재전송하여 인가되지 않은 사항에 접근
- 메시지변조(Modification of messages): 적법한 메시지 일부를 변경하거나, 비인가 메시지 효과를 내기 위하여 메시지를 지연시키거나 순서를 뒤바꾸는 행위
- 서비스 거부(Denial of service): 통신 설비나 서비스가 정상 운용되거나 관리되지 못하도록 함

보안 서비스(Security Services)

보안 서비스는 다음과 같이 정의된다.

- X.800 정의: 시스템이나 데이터 전달에 대한 적절한 보안을 보장하기 위하여 데이터 통신 시스템의 프로토콜 계층에서 제공되는 서비스
- RFC 4949: 시스템 자원에 대한 특정한 종류의 보호를 하기 위하여 시스템에 의하여 제공되는 프로세스 또는 통신 서비스

X.800에 따르면 보안 서비스에는 인증(Authentication), 접근제어(Access control), 데이터 기밀성(Data confidentiality), 데이터 무결성(Data integrity), 부인봉쇄(Nonrepudiation), 가용성(Availability)을 포함한다.

- **인증(Authentication)**

  통신이 검증되었다는 것을 확인해주는 서비스로 당사자 인증과 데이터 출처 인증으로 구분된다. 단일 메시지를 수신한 경우 수신자는 신뢰할 수 있는 출처에서의 메시지인지 궁금하다. 금융 서비스 등에서 문자로 인증번호를 수신한 경우가 좋은 예가 된다. 또한 주고 받는 메시지의 경우는 쌍방 인증을 보장해야 하며 연결 상태에서 3자의 위장 개입을 차단했는지를 보장해야 한다.

- **접근 제어(Access Control)**

  통신 링크를 통하여 호스트 시스템이나 애플리케이션에 대한 접속 제한 및 제어를 제공하는 서비스로 비 인가자의 자원 이용을 차단하는 목적이다. 이를 위해서는 자원에 접근 가능한 사람, 접근 조건, 접근 내역 등을 제어해야 하며 액세스 획득을 시도하는 엔티티는 먼저 신분을 확인하고 액세스 권한은 개별적으로 부여해야 한다.

- **데이터 기밀성(Data Integrity)**

  비 인가된 노출로부터 데이터 보호하는 서비스로 소극적 공격에서 전송된 데이터를 보호하는 목적이다. 분석 공격으로부터 트래픽을 보호하여 공격자가 통신 설비의 트래픽에 대한 발신지와 목적지, 빈도, 길이 또는 다른 특성을 관찰할 수 없게 하는 기능을 제공한다.

- **데이터 무결성(Data Integrity)**

  수신 데이터가 인가된 송신자가 전송한 것임을 보장하는 서비스로 수정, 추가, 제거, 재전송이 없음을 확인해 준다.

- **부인봉쇄(non-repudiation)**

  통신 당사자 중 하나가 통신의 일부 또는 전체에 참여한 사실을 부인하는 행위를 차단하는 서비스로

  - 부인봉쇄-출처(Nonrepudiation, Origin) : 특정 당사자로부터 메시지가 전송된 것을 입증

  - 부인봉쇄-목적지((Nonrepudiation, Destination) : 특정 당사자에게 메시지가 수신되었음을 입증

- **가용성(Availability)**

  인가자의 요구에 따라 시스템이나 시스템 자원에 접속할 수 있는 속성으로 시스템의 성능 유지 조건과 관련한 서비스로

  - 시스템이 가용성을 보장하도록 보호: 시스템 자원에 대한 적절한 관리와 제어 요구

  - 서비스 거부 공격에 대한 대응 서비스

- **보안 메커니즘(Security Mechanisms: X.800)**

  보안 메커니즘은 보안 공격을 탐지, 차단, 또는 복구를 위해 설계된 보안 프로세스나 보안 프로세스를 수행하는 디바이스를 의미한다. 보안 메커니즘은 특정 프로토콜 계층(TCP/응용계층)에 적용되는 특정 보안 메커니즘과 특정 프로토콜 계층/보안 서비스에 국한되지 않은 범용 메커니즘으로 분류한다.

- **보안 메커니즘(Security Mechanisms: X.800)**

  - 특정 보안 메커니즘:

  . 암호화(Encipherment), 디지털 서명(Digital Signature), 접근통제(Access Control),

  데이터 무결성(Data Integrity), 인증 교환(Authentication Exchange),

  트래픽 패딩(Traffic Padding), 경로 제어(Routing Control), 공증(Notarization)

  - 범용 보안 메커니즘:

  . 신뢰받는 기능(Trusted Functionality), 보안 레이블(Security Label),

  사건 탐지(Event Detection), 보안감사 추적(Security Audit Trail),

  보안 복구(Security Recovery)

02. 해킹의 이해

해킹의 진화

- 1986년 1월에 "brain"이하는 세계 최초의 바이러스 등장하였다. 이것은 플로피 디스코를 통해 전파되었지만 그 이후의 바이러스들은 주로 이메일에 첨부되어 전파되었다. 1994년 넷스케이프라는 웹 브라우저가 등장하면서 해킹도구는 개발하여 인터넷에 공개되기 시작하였고 이를 통해 개인정보를 캐고 은행 컴퓨터의 계좌정보를 변조하는데 악용되었다. 이것은 해커의 의미를 언론에서 악의적으로 표현하는 계기가 되었다.
- 2000년대에 들어서 컴퓨터가 대중화되면서 대중이 컴퓨터 바이러스를 인지하게 되었고 PC에 방화벽과 백신을 설치하여 해킹에 대비하기 시작하였다. 하지만 2002년 2월 CNN 및 아마존이 분산 서비스 거부 공격을 받아 몇 시간동안 마비되는 사태가 벌어지는 등 웜과 바이러스에 의한 대형 피해가 속출하였다. 일명 러브버그(Love Bug)라고 불리는 바이러스는 이메일에 첨부되어 전송되었는데, 수신자가 이메일의 첨부를 클릭할 경우 수신자 컴퓨터에 저장된 다른 이메일 계정으로 메일이 복제되어 전송되면서 87.5억 달러의 손실이 발생한 것으로 추정되었다. 한국에서는 2003년 1월 25일 마이크로소프트사의 SQL-2000 서버를 공격하는 슬래머 웜으로 인한 전국의 네트워크가 마비되는 사건이 발생하기도 하였다. 일명 1.25 대란인 것이다.
- 2003년 이후에는 웹이 급속도로 확산되면서 웹서버의 OS나 서버 애플리케이션 취약점을 악용한 웹 애플리케이션을 노린 공격이 증가하였다. 즉 웹을 통해 개인정보 유출과 도용이 극성을 부리기 시작하였다. 이것은 금융 피해로 이어졌다. 2007년에는 공인인증서 유출로 시중 은행에서 현금을 불법 인출하는 사건이 발생하는 등 해킹을 통해 자신의 능력을 과시하는 단계를 지나 금전을 목적으로 진화한 것이다.
- 2010년대에는 사이버 공격으로 인해 사회적 문제가 제기된 시기이다. 2011년 4월에는 사회적 혼란을 목적으로 북한 소행의 농협 사이버 테러가 발생하여 대규모의 데이터가 삭제되기도 하였다. 아울러 이 시기에는 지능형 해킹 공격(APT: Advanced Persistent Threat)으로 금전적 가치뿐만 아니라 정치적 가치를 노리는 사건이 발생하였다.

- 또한 WiFi, 3G 및 LTE 망을 이용하는 스마트폰은 다양한 경로를 통해 공격이 가능한 최상의 해킹도구이자 해킹 대상이 된 시기이다. 예를 들어 무선랜 해킹도구가 설치된 스마트폰을 공격대상의 기업으로 존재하지 않은 직원 명의로 택배를 보내게 되면 그 택배가 기업 내에서 반송될 때까지 방치될 수 있는데, 그 기간 동안 기업 내부의 무선 네트워크를 해킹하는데 택배내의 스마트폰을 이용하는 것이다.
- 정리하여 보면 해킹의 진화의 이면에는 기술발전의 영향도 있지만 비즈니스 이해관계가 밀접하게 연관되어 있는 것이다. 즉 해킹을 통한 수익모델의 진화에 따라 사이버 범죄가 점점 산업화, 정치화 되고 있다. 즉, 과거에는 연구 유형의 해킹 비즈니스(Research-as-a Service)로 이 분야에 속한 사람들을 화이트 해커라 칭하였으며, 이들은 공개되지 않은 취약점이나 공격 수법을 무료 공개하거나 상업적으로 판매하기도 하였다. 보안에 민감한 기업에서는 버그 바운티(Bug Bounty)라는 제도를 통하여 취약점의 발견에 대한 대가를 지급하고 있다. 페이스북의 경우에는 버그 바운티 제도를 통하여 2013년 1인당 평균 2204달러(약 228만원), 총 150만 달러(약 16억원) 지급하였다.
- 화이트 해커가 크래커 영역으로 전환되는 단계에서는 해킹 툴을 판매(Crime-as-a-Service)하기 시작하였는데, 예를 들어 사이버 범죄용 특수 툴, 악성 프로그램 제작 판매 및 공격수법 판매 등을 하였다. 이후 보다 많은 금전을 획득하는 목적으로 산업화되면서 청부해킹 서비스(Hacking-as-a Service) 형태로 금전을 대가로 하여 특정 이메일의 패스워드 파괴하거나 특정 사이트 대상의 디도스 공격을 하는 것이 일반화 되었다. 최근 몇 년간에는 개인이나 기업 소유의 저장된 중요 정보를 암호화시킨 후 복호화에 대한 대가를 요구하며 협박하는 랜섬웨어(ransomware)가 조직화 되면서 국제적인 이슈가 되고 있다. 랜섬웨어에 대해서는 7차시에서 별도로 학습하기로 한다.

해킹 프로세스

- 현재 우리나라의 정보통신망법에서는 해킹을 다음과 같이 정의하고 있다.

  - 정당한 접근권한 없이 또는 허용 접근권한을 초과하여 정보통신시스템에 침입하는 행위
  - 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생시키는 행위

  즉 앞서 학습한 사이버 보안 목적인 기밀성, 무결성, 가용성, 인증 및 책임성 달성에 영향을 주는 일련의 행위가 해킹인 것이다. 따라서 해킹 과정을 파악하게 되면 해킹에 효과적인 대응방안을 이해하는데 도움이 된다. 일반적인 해킹은 6단계의 과정을 통해서 진행된다.

  1. 정보 수집 단계 (Information Gathering)
  2. 취약점 분석 단계(Vulnerability Analysis)
  3. 불법접근, 권한획득 단계 (Acquiring Access Rights & Escalating Privilege)
  4. 정보수집도구 설치단계(Installing Backdoor)
  5. 불법행위 수행단계
  6. 흔적 제거 (Covering Track)

- 공격자는 공격대상을 선정하고 공격 대상에 대한 입체적인 정보를 수집하는 단계로 해킹을 시작한다. 즉, 공격대상의 관련기사, 회사 주소, 전화번호 및 담당자의 e-mail 주소를 포함하여 공격 대상에서 제공 서비스와 시스템, 사용 중인 포트 등을 분석하고 운영체제와 네트워크 관련 정보를 수집한다.
- 취약점 분석 단계에서는 정보 수집 단계에서 얻은 정보를 바탕으로 공격 대상에 대한 취약점을 점검하여 공격 대상에서 제공하는 서비스의 공격 가능한 취약점을 파악한다. 즉, 취약점 스캐닝은 컴퓨터, 네트워크 및 통신 장비의 보안 취약성을 스캔하여 발견된 취약점에 대한 패치를 하지 않은 경우에는 그것을 이용하여 공격을 위한 시나리오 구성에 활용한다. 취약점은 네트워크와 소프트웨어는 물론 인적 분야에서도 존재한다.

  - 네트워크 취약점

  . 기업 네트워크, WAN 또는 인터넷 상의 취약점

  . DDoS에 이용되는 네트워크 프로토콜 취약점, 통신 링크 방해

  - 소프트웨어 취약점

  . 응용 프로그램, 유틸리티, 운영체제코드의 취약점

  . 웹 서버 소프트웨어 취약점

  - 인적 취약점

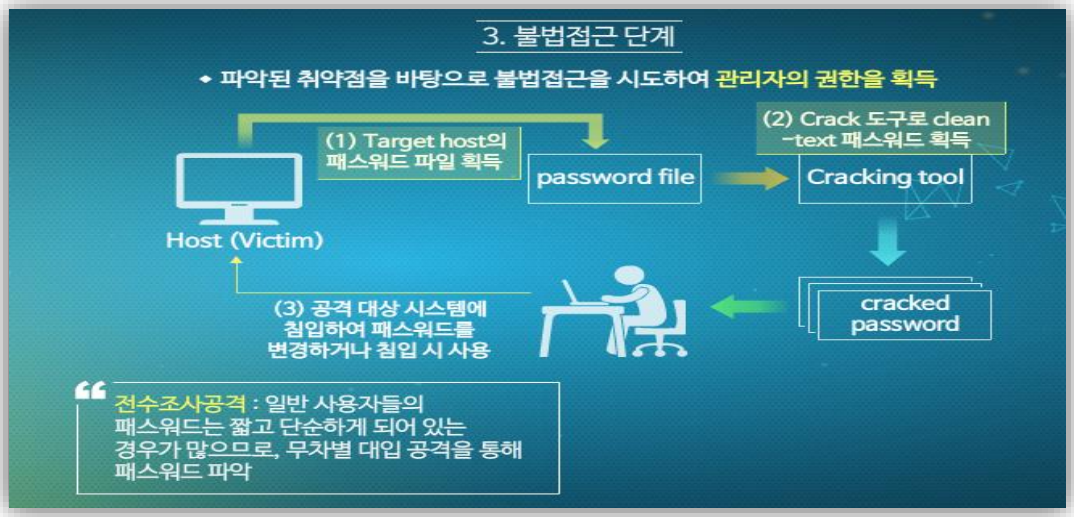
  . 인적 요소나 외부인에 의한 취약점

  . 사회 공학, 인적 오류, 신뢰 받는 내부인

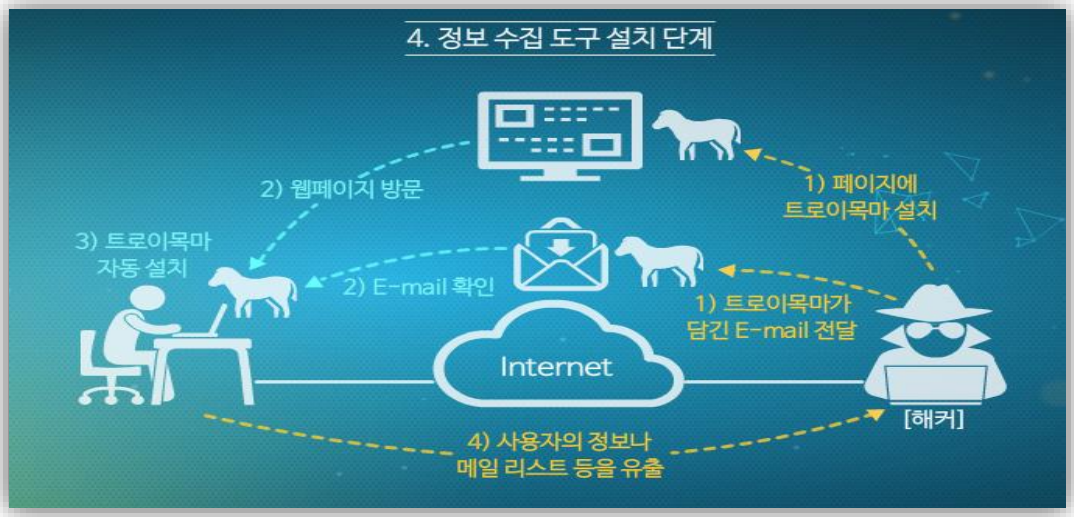
  불법 접근 단계에서는 파악된 취약점 바탕으로 불법접근을 시도하여 관리자의 권한을 획득하거나 접근 권한의 상승을 목적으로 아래와 같은 행위를 한다.

  - 전수조사공격(Brute force attack) : 일반 사용자들의 패스워드는 짧고 단순하게 되어 있는 경우가 많으므로, 무차별 대입 공격을 통해 패스워드를 파악(아래 그림의 1, 2과정)

  - 일반 사용자의 계정과 패스워드를 통해 시스템에 로그 온한 후, 취약점을 통해 root나 관리자(administrator)계정으로 권한 상승



- 정보수집 도구 설치 단계에서는 스니핑(sniffing) 도구, 악성 프로그램, 백도어, 루트킷 등을 설치한다(아래 그림 참조). 즉, 해커는 트로이목마가 담긴 이메일을 전송하거나 해킹한 홈페이지에 트로이 목마를 설치한다. 보안이 취약한 PC 사용자가 웹 페이지를 방문하거나 이메일을 확인하면서 트로이 목마를 자동 설치하면 사용자의 정보나 메일 리스트 등이 유출된다.



- 불법행위 수행 단계에서는 정보 유출이나 시스템 파괴 등의 불법 행위를 수행한다.
- 끝으로 해킹흔적 삭제 단계에서는 시스템의 관리자 권한을 획득하게 되면 공격관련 로그 기록을 삭제하여 기존 관리자가 알아채지 못하게 로그 파일을 변조한다. 또한 접근 로그 및 기타 보안 관련 로그들을 삭제함으로써 향후에 감사를 불가능하게도 만든다. 이 단계에서는 수동으로 로그 파일을 찾아 삭제하기도 하지만 흔적을 자동으로 지워주는 해킹 툴을 설치하기도 한다.