4. 보안 공격 유형

보안 공격은 특정 조직의 정보보호를 저해하는 모든 행위이다.

	공격 유형	특 징
소극적 공격 (passive attack)	• **가로채기(도청)** • **트래픽 분석(감시)**	• 직접적인 피해를 주지는 않는다. • 통신상 변화가 없으므로 탐지 곤란 • 탐지하기 보다는 예방이 필요하다.
적극적 공격 (active attack)	• 가로막기(방해) • 메시지 변조(수정) • 위조(가장, 신분위장) • 서비스 거부 • 재전송(replay, 재연)	• 직접적인 피해를 준다. • 실제로 데이터를 변경하기도 한다. • 모든 자원에 대한 예방은 매우 어렵다. • 모든 자원에 대한 지속적 보호는 불가능 • 탐지 및 복구가 필요하다.

• 소극적 공격은 **수동적** 공격, 적극적 공격은 **능동적** 공격이라고도 한다.

(1) 소극적 공격(passive attack) – 수동적 공격

① 가로채기(interception, **도청**)
- 불법적인 접근, 하지만, 수신자는 정보를 받는다.

② 트래픽 분석(traffic analysis)
- 트래픽 분석은 송수신되는 데이터 자체 외의 **다른 정보**를 **유추**하는 공격이다
- 트래픽 분석은 송수신자 신분, 통신시간 등을 주기적으로 관찰/분석하는 행위이다.

(2) 적극적 공격(active attack) – 능동적 공격

① 가로막기(interruption, **방해**)
- 가용성 침해 요인, 수신자가 정보를 받을 수 없다.
- 시스템이 파괴되거나 통신을 할 수 없는 상황이다.

② 불법적인 메시지 변조(modification, 수정)
- 무결성 침해 요인, 수신자는 내용이 수정된 정보를 받는다.

③ 위조(fabrication), 가장(masquerading) – 스푸핑(spoofing)
- 무결성 침해 요인, 신분 위장, 거짓 정보 추가(위조문서)
- 비인가자가 네트워크상에 위조된 메시지를 삽입(인증에 대한 공격)

④ 서비스 거부 공격
- 가용성 침해 요인, 특정 목표물을 무력화 시킨다.

탐구

기본 용어 정리

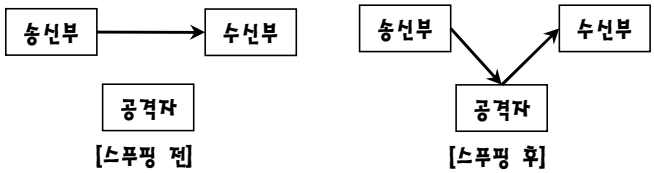
◉ 위조(위장, 가장) / 도청(가로채기)

한국어	영 어	사전적 의미
위조(위장, 가장)	스푸핑(spoofing)	속이다, 사기를 치다, 위장하다.
도청(가로채기)	스니핑(sniffing)	킁킁거리며 냄새를 맡는다. 엿보기
	스누핑(snooping)	염탐하다. 기웃거리다. 비인가 접근

• 시험에서는 주로 "스니핑(sniffing) / 스푸핑(spoofing)"으로 출제되었다.

◉ 스푸핑(spoofing) - 예 : ARP 스푸핑

• 먼저, 영어 단어 spoofing은 '속이다, **사기치다**, 위장하다'라는 뜻이다.
• 네트워크상에서 스푸핑 대상은 'IP주소, MAC 주소, 포트번호, DNS 등' 네트워크에서 통신하는 것과 관련된 모든 것이 될 수 있다.
• 따라서, 스푸핑은 속임수를 이용한 공격 기법을 총칭한다.
• 예를 들면, 스푸핑은 공격자 컴퓨터를 경유하지 않는 패킷을 의도적으로 공격자 컴퓨터를 경유하도록 한다.



• ARP 스푸핑은 송수신자의 MAC 주소를 **공격자의 MAC 주소로 변경**하는 것이다.

◉ 스니핑(sniffing) / 스누핑(snooping)

• sniffing은 '킁킁거리며 냄새를 맡는다**(도청, 가로채기)**'라는 뜻이다. → 훔치다.
• 스니퍼(sniffer)는 '네트워크에 흐르는 트래픽을 엿듣는 도청장치 프로그램'이다.
• 패킷(packet) 스니핑은 네트워크상에 흐르는 패킷을 도청하는 것이다.
• 예 : 통신망에 접속하기 위해 아이디와 비밀번호를 입력할 때 이를 도청할 수 있다.
• 스니핑(sniffing)과 비슷한 단어로 스누핑(snooping)이 있다.
• snooping의 사전적 의미는 "염탐하다, 기웃거리다"라는 뜻이다.

◉ **피싱(phishing) = private + data + fishing**

- phishing은 fishing(낚시)에서 발음이 비슷하도록 변형한 것이다.
- '정보의 바다' 인터넷에서 **스팸메일을 미끼**로 개인 사용자를 '낚는' 것을 비유한 것이다.
- 피싱은 스푸핑(spoofing) 원리이다.
- 피싱은 송신자(공격자)가 신원을 감춘 스팸메일을 보낸다.
  → 이를 이용하여 수신자의 개인정보를 빼내서 범죄에 이용하는 인터넷 범죄 수법이다.
- 피싱은 주로 금융기관을 사칭하거나 이벤트, 설문조사 등을 빙자해서 개인정보를 요구한다.
  → 신용카드나 통장 계좌에 문제가 있다는 구실로 계좌번호와 비밀번호 등을 요구한다.
  → 이벤트, 설문조사 등을 빙자해서 선물 등을 주겠다고 개인정보를 요구하기도 한다.

◉ **파밍(pharming)**

- 파밍은 피싱에서 더 나아간 해킹 기술이다. 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 은행계좌, 신용카드정보, 주민등록번호 같은 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 정상 사이트의 **도메인이름**을 정확히 입력해도 가짜 사이트로 연결되는 해킹 기술이다.
- 파밍은 **정확한 도메인이름을 입력**해도 **가짜 웹서버**에 접속되어 개인정보가 도용되는 것이다.
- 파밍은 이용자 PC의 호스트(hosts) 파일을 변조하는 악성코드에 감염되어 발생한다.
- 파밍 예방은 hosts 파일에 은행, 공공기관 등의 도메인이 추가되어 있는지 확인하면 된다.
- 파밍은 호스트(hosts) 파일에 은행, 공공기관의 도메인이 추가되어 있는지 확인하면 된다.
- hosts 파일을 메모장 프로그램을 이용해서 열어보면 변조된 것을 확인할 수 있다.
- 파밍은 한국 형법상 개인정보수집 위반죄, 변작죄, 절도죄, 사기죄 등이 성립될 수 있다.

◉ **스미싱(smishing, SMS phishing) - 문자메시지 피싱**

- 문자메시지를 이용한 피싱이다. [스미싱(smishing) = 문자메시지(SMS) + 피싱(phising)]
- 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 가장하여 개인정보를 요구한다.
- 스마트폰이 대중적으로 보급되자 부각되었다.
- 피싱(phishing)은 스팸메일을 이용한 인터넷 신종 개인정보 탈취 범죄이다.
- 보이스 피싱 등 피싱의 유형은 다양하다.

◉ **스피어 피싱(spear phishing)**

- 스피어 피싱의 명칭은 작살로 물고기를 잡다 라는 뜻에서 유래 되었다.
- 영어 단어 스피어(Spear)는 작살, 투창을 뜻한다.
- 스피어 피싱은 **불특정 다수가 아닌 특정인을 목표**로 정해 맞춤형 공격을 진행한다.
- 스피어 피싱은 공격 대상이 극히 제한적이며, 정교한 공격이 가능하다.
- 스피어 피싱은 사회공학적 해킹의 한 기법이다.
- 스피어 피싱의 대상은 회사 고위간부나 국가의 중요 업무를 담당하고 있는 사람이다.
- 그들이 흥미를 끌만한 이메일 등을 통하여 공격대상의 클릭을 유도한다.

◉ **중간자 공격(man in the middle attack, MITM)**

• 통신 두 당사자 중간에서 정보를 **도청**하거나 그 **내용을 바꿔치는** 보안 공격

◉ **중간자 공격(man in the middle attack, MITM) 예방**

One-time pad 암호 (일회용 암호)	• 한 번 사용한 비밀키는 버리므로 일회용암호라 한다. • One-time pad 암호는 중간자 공격에 면역되어 있다.
공개키 기반구조 (PKI)	• PKI는 상호인증을 통한 방어이다. • 대부분의 암호 프로토콜은 중간자 공격을 막기 위하여 인증을 사용한다.
양자암호 (quantum cryptography)	• 양자의 역학적 특성을 이용한 암호 기술이다. • 암호체계가 비가역적인 물리학적 자연현상에 기반을 두고 있다. • 양자암호의 큰 보안성은 측정이 단 1회만 허용되는 것이다. • 양자암호는 최초 측정이 잘못되면 두 번째 측정부터는 정확한 측정이 불가능하다. • 신호 측정에 실수를 하게 되면, 신호가 왜곡되어 도청자의 존재가 발각된다.

◉ **재전송(replaying, 재연, 재생)**

• 재전송은 유효한 데이터를 중간에 몰래 낚아채어 나중에 이를 **그대로 재사용/재전송**하는 것이다.
• 재전송은 부주의, 중간자 공격 등으로 유출된 암호나 개인정보 등을 재사용하는 것이다.
• 캡처된 정보를 "재생"하는 디지털 보안시스템에 대해 공격하는 것으로, 수신시스템으로 하여금 공격자에게 오리지널, 합법적인 정보와 관련된 모든 자원을 제공하도록 강제하고 있다.
• 재전송은 중간자 공격에 속한다.

〈재전송 공격 예〉

• 은행 송금 메시지를 공격자가 **도청**하고, 나중에 이 메시지를 은행에 다시 보내어 돈을 **이중**으로 **송금**하도록 한다.
• PDF 문서에 비용을 지불하고, 다운로드 페이지를 전달받은 웹 사용자들은 다운로드 URL을 자신의 브라우저 스크린으로부터 캡처한 후 친구들에게 전자우편으로 전송하여 그 문서의 다른 **복사본**을 얻을 수 있도록 한다.

〈재전송 공격 예방〉

• 시스템은 매번 다른 **인증**을 생성하거나 인증 속에 사용자 관련 정보를 넣음으로써 재생 공격을 잘 방어할 수 있도록 만들 수 있다.

◉ 부인(repudiation) / 부인방지(부인봉쇄)

- **부인**은 거짓말을 하는 것이다.
- **부인봉쇄**는 거짓말을 할 때, 거짓말을 못하도록 보장하는 개념이다.(전자서명 이용)
- 부인봉쇄는 이미 발생한 통신(송수신)의 부인을 막기 위한 통신의 한 속성이다.
- 부인봉쇄는 송신자를 보호하기 위해서는 수신자의 수신 증거를 제공하고
  수신자를 보호하기 위해서는 송신자의 송신 증거를 제공하는 보안 서비스이다.
- 인터넷 쇼핑몰에서 상품을 구입하고 전자 결재를 하였는데,
  나중에 상인이 결재 받은 사실을 부인하고 결재할 것을 요청하는 경우
- 은행 고객이 은행에게 제3자에게 돈을 송금할 것을 요청하고,
  나중에 송금 요청한 사실을 부인하는 경우

〈부인이 발생하는 경우〉

- 수신자는 메시지를 받았다고 주장하지만, 송신자는 메시지를 보내지 않았다고 주장
- 수신자가 받았다고 주장하는 내용과는 다른 메시지를 송신자가 보냈다고 주장
- 송신자는 메시지를 보냈다고 주장하지만, 수신자는 메시지를 받지 않았다고 주장
- 송신자가 보냈다고 주장하는 내용과는 다른 메시지를 수신자가 받았다고 주장
- 송수신자는 메시지를 송수신한 날짜 및 시간을 서로 다르게 주장

◉ 백도어(back door) / 트랩도어(trap door)

- 백도어와 트랩도어는 프로그램의 일종으로 같은 의미로 사용된다.
- 백도어는 **시스템 보안이 제거된 비밀통로**를 지칭한다.
- 백도어는 시스템 설계자가 고의로 만들어 놓은 시스템의 비밀통로이다.
- 백도어는 유지보수 등을 위한 접근 편의를 위해 만들어 놓은 시스템의 비밀통로이다.
- 프로그램 개발에서 코드 내에 백도어라는 중단 부분을 설정하여 보수할 수 있게 한다.
- 백도어는 최종 단계에서 삭제되어야 한다. 남아 있으면 범죄에 악용되기도 한다.
- 초기에는 백도어는 주로 프로그래머들이 로그인 등 편의를 위해 만들었다.
  → 그 후, 해커들이 백도어를 만들어 공격 컴퓨터 침입 수단으로 사용하고 있다.
- 백도어 프로그램은 시스템 관리자나 프로그래머가 컴퓨터에 로그인해 들어가는 과정을 쉽게 하려고 변칙적으로 개발한 프로그램이다.
  → 예를 들면, 네트워크상에서 다른 컴퓨터로 접속할 때 단축키('A', 'F9' 등)를 누르면 바로 해당 컴퓨터에 접속할 수 있도록 한 것이다.
  → 이를 제3자가 알게 되면 시스템 관리자의 권한을 가지므로 보안에 문제가 된다.

기출문제 분석

1. 능동적 공격에 해당하는 것만을 모두 고르면? [2021년 국가 9급]

ㄱ. 도청 ㄴ. 서비스 거부
ㄷ. 트래픽 분석 ㄹ. 메시지 변조

---

① ㄱ, ㄷ ② ㄴ, ㄷ ③ ㄴ, ㄹ ④ ㄷ, ㄹ

♤ 보안 공격

	공격 유형	특 징
수동적 공격 (passive attack)	• 가로채기(도청) • 트래픽 분석(감시)	• 직접적인 피해를 주지는 않는다. • 통신상 변화가 없으므로 탐지 곤란 • 탐지하기 보다는 예방이 필요하다.
능동적 공격 (active attack)	• 가로막기(방해) • 메시지 변조(수정) • 위조(가장, 신분위장) • 서비스 거부 • 재전송(replay, 재연)	• 직접적인 피해를 준다. • 실제로 데이터를 변경하기도 한다. • 모든 자원에 대한 예방은 매우 어렵다. • 모든 자원에 대한 지속적 보호는 불가능 • 탐지 및 복구가 필요하다.

정답 : ③

2. 보안 공격에 대한 설명으로 옳지 않은 것은? [2015년 국가 7급]

① 소극적 공격은 시스템의 정보를 알아내거나 악용하지만, 시스템 자원에 영향을 주지 않는다.
② 적극적 공격은 실제로 데이터를 변경하지 않기 때문에 탐지하기 매우 어렵다.
③ 소극적 공격의 유형에는 메시지 내용 공개, 트래픽 분석이 있다.
④ 적극적 공격의 유형에는 신분위장, 서비스 거부, 재전송이 있다.

♤ 보안 공격

• 적극적 공격은 실제로 데이터를 변경하지 않기 때문에 탐지하기 매우 어렵다.(×)
→ 적극적 공격은 실제로 데이터를 변경하기도 한다.

정답 : ②

3. 다음 중 트래픽 분석(traffic analysis)에 대한 설명으로 가장 옳은 것은? [2022년 군무원 7급]

① 사용자가 보낸 메시지 사본을 획득하여 나중에 그 메시지를 사용하기 위한 목적으로 이용하는 소극적 공격이다.
② 시스템의 서비스를 느리게 하거나 완전히 차단하는 적극적 공격이다.
③ 송수신되는 데이터를 가로채거나 획득 후 정보를 조작하는 적극적 공격이다.
④ 송수신되는 데이터 자체 외의 다른 정보를 유추하는 소극적 공격이다.

♤ **보안 공격 유형**

① 사용자가 보낸 메시지 사본을 획득하여 **나중에 그 메시지를 사용**하기 위한 목적으로 이용하는 **소극적 공격**이다.(×) → **재전송.적극적 공격**
② 시스템의 서비스를 느리게 하거나 **완전히 차단**하는 적극적 공격이다.(×) → **가로막기.적극적 공격**
③ 송수신되는 데이터를 **가로채거**나 획득 후 **정보를 조작**하는 적극적 공격이다.(×)
→ **가로채기.소극적 공격, 위조.적극적 공격**
④ 송수신되는 데이터 자체 외의 다른 정보를 유추하는 소극적 공격이다.(○)
→ **트래픽분석.소극적 공격**

정답 : ④

4. 보안 공격 유형에는 적극적 공격과 소극적 공격이 있다. 다음 중 공격 유형이 다른 하나는? [2022년 지방 9급]

① 메시지 내용 공개(release of message contents)
② 신분 위장(masquerade)
③ 메시지 수정(modification of message)
④ 서비스 거부(denial of service)

♤ **적극적 공격과 소극적 공격**

	공격 유형
소극적 공격 (passive attack)	• 가로채기(도청) – 메시지 내용 공개 • 트래픽 분석(감시)
적극적 공격 (active attack)	• 가로막기(방해), 메시지 변조(수정) • 위조(가장, 신분위장) • 서비스 거부, 재전송(replay, 재연)

정답 : ①

5. 보안 공격 중 적극적 보안 공격의 종류가 아닌 것은? [2014년 지방 9급]

① 신분위장(masquerade) : 하나의 실체가 다른 실체로 행세를 한다.
② 재전송(replay) : 데이터를 획득하여 비인가된 효과를 얻기 위하여 재전송한다.
③ 메시지 내용 공개(release of message contents) : 전화통화, 전자우편 메시지, 전송 파일 등에 기밀 정보가 포함되어 있으므로 공격자가 전송 내용을 탐지하지 못하도록 예방해야 한다.
④ 서비스 거부(denial of service) : 통신 설비가 정상적으로 사용 및 관리되지 못하게 방해한다.

♤ **보안 공격**

---

③ 메시지 내용 공개(release of message contents) : 전화통화, 전자우편 메시지, 전송 파일 등에 기밀 정보가 포함되어 있으므로 공격자가 전송 내용을 탐지하지 못하도록 예방해야 한다.
→ "가로채기(도청)"에 해당하는 내용이다. - 소극적 공격

정답 : ③

6. 스미싱 공격에 대한 설명으로 옳지 않은 것은? [2021년 지방 9급]

① 공격자는 주로 앱을 사용하여 공격한다.
② 스미싱은 개인정보를 빼내는 사기 수법이다.
③ 공격자는 사용자가 제대로 된 url을 입력하여도 원래 사이트와 유사한 위장 사이트로 접속시킨다.
④ 공격자는 문자 메시지 링크를 이용한다.

♤ **스미싱 공격**

• 공격자는 사용자가 제대로 된 **url**을 입력하여도 원래 사이트와 유사한 **위장 사이트로 접속**시킨다.**(×)** → **파밍** 공격에 대한 설명이다.

◉ **스미싱(smishing, SMS phishing) - 문자메시지 피싱**

• 문자메시지를 이용한 피싱이다. [스미싱(smishing) = 문자메시지(SMS) + 피싱(phising)]
• 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 가장하여 개인정보를 요구한다.
• 스마트폰이 대중적으로 보급되자 부각되었다.
• 피싱(phishing)은 스팸메일을 이용한 인터넷 신종 개인정보 탈취 범죄이다.
• 보이스 피싱 등 피싱의 유형은 다양하다.

정답 : ③

7. 보안 침해 사고에 대한 설명으로 옳은 것은? [2017년 국가 9급]

① 크라임웨어는 온라인상에서 해당 소프트웨어를 실행하는 사용자가 알지 못하게 불법적인 행동 및 동작을 하도록 만들어진 프로그램을 말한다.

② 스니핑은 적극적 공격으로 백도어 등의 프로그램을 사용하여 네트워크상의 남의 패킷 정보를 도청하는 해킹 유형의 하나이다.

③ 파밍은 정상적으로 사용자들이 접속하는 도메인 이름과 철자가 유사한 도메인 이름을 사용하여 위장 홈페이지를 만든 뒤 사용자로 하여금 위장된 사이트로 접속하도록 한 후 개인정보를 빼내는 공격 기법이다.

④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.

♤ **크라임웨어(crimeware) – 신조어**

- 영어 단어 crime은 범죄를 의미한다.
- 크라임웨어는 개인정보 유출, 피싱 등 온라인 범죄행위를 용이하게 하는 악성코드이다.
- 온라인상에서 불법 활동을 조장하기 위해 만들어진 컴퓨터 프로그램들이다.
- 예 : 스파이웨어, 키로거, 브라우저 하이재커 등을 말한다.
- 크라임웨어를 이용하여 중요한 개인 금융 정보 또는 인증 정보를 수집할 수 있다.

◉ **틀린 이유**

② 스니핑은 **적극적** 공격으로 백도어 등의 프로그램을 사용하여 네트워크상의 남의 패킷 정보를 도청하는 해킹 유형의 하나이다.**(×)** → 스니핑은 **소극적** 공격

③ 파밍은 정상적으로 사용자들이 접속하는 도메인 이름과 철자가 **유사한 도메인** 이름을 사용하여 위장 홈페이지를 만든 뒤 사용자로 하여금 위장된 사이트로 접속하도록 한 후 개인정보를 빼내는 공격 기법이다.**(×)**

→ 파밍은 인터넷 사용자가 자신의 웹 브라우저에서 **정확한 도메인** 이름을 입력해도 가짜 웹 서버에 접속되어 개인정보가 도용되는 것이다.

④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 **도메인 자체를 탈취**하는 공격 기법이다.**(×)** → 피싱은 **스푸핑**(spoofing) 원리이다.

→ 피싱은 주로 금융기관을 사칭하여 신용카드나 통장 계좌에 문제가 있다는 구실로 계좌번호와 비밀번호, 신상정보 등을 요구한다.

정답 : ①

8. 능동적 공격으로 가장 옳지 않은 것은? [2018년 서울 9급]

① 재전송 ② 트래픽 분석
③ 신분위장 ④ 메시지 변조

♤ **보안 공격 유형**

• 소극적 공격 : 트래픽 분석, 가로채기(도청)

정답 : ②

9. 공격 유형에 관한 설명으로 옳지 않은 것은? [2017년 국가 정보보호 9급]

① 사회공학적 공격은 신뢰 관계나 인간의 심리를 이용하여 중요한 정보를 획득하는 것이다.
② 무차별(brute force) 공격은 특정 값을 찾아내기 위해 가능한 모든 조합을 시도하는 공격이다.
③ 스니핑은 네트워크상에서 다른 사용자들의 트래픽을 도청하는 것이다.
④ 재연(replay) 공격은 두 개체 간의 패킷을 중간에서 가로채서 변조하여 전송함으로써 정당한 사용자로 가장하는 공격이다.

♤ **재연(replay) 공격 - 재생 공격, 재전송 공격**

◉ **재생 공격 정의 - 용어사전 참조**

• 캡처된 정보를 "재생"하는 디지털 보안 시스템에 대해 공격하는 것으로, 수신 시스템으로 하여금 공격자에게 오리지널, 합법적인 정보와 관련된 모든 자원을 제공하도록 강제하고 있다.
→ 전형적으로 일종의 디지털 인증을 하는 것이다.
→ 유효한 데이터를 중간에 몰래 낚아채어 나중에 이를 **그대로 재사용/재전송**하는 것
→ 부주의, 중간자 공격 등으로 유출된 암호나 개인정보 등을 재사용하는 것이다.

◉ **재생 공격 예**

이중 송금	은행 송금 메시지를 공격자가 **도청**하고, 나중에 이 메시지를 은행에 다시 보내어 돈을 **이중**으로 **송금**하도록 한다.
불법 복사	PDF 문서에 비용을 지불하고, 다운로드 페이지를 전달받은 웹 사용자들은 다운로드 URL을 자신의 브라우저 스크린으로부터 캡처한 후 친구들에게 전자우편으로 전송하여 그 문서의 다른 **복사본**을 얻을 수 있도록 한다.

정답 : ④

10. 패스워드를 이용해서 원격 사용자를 인증하는 경우, 호스트는 비표라는 일회성 임의 숫자 r를 생성하고 이와 함께 두 함수 h()와 f()를 사용자에게 제시한다. 사용자는 이에 대한 응답으로 f(r', h(P'))를 반환한다. 호스트는 r'=r, h(P')=h(사용자 패스워드)의 여부를 판단하여 인증을 완료한다. 이때, r를 사용하는 것은 어떤 공격에 대비하기 위한 것인가? [2019년 국가 7급]

① 전사공격(brute-force attack)
② 트래픽 스니핑 공격(traffic sniffing attack)
③ 패스워드 사전공격(password dictionary attack)
④ 재전송공격(replay attack)

♤ **패스워드를 이용한 원격 사용자를 인증 / 재전송공격 방지**

- 일회성 임의 숫자 r를 생성하여 원격 사용자 인증은 재전송공격 방지를 위한 것이다.
- 악의적인 제3자에게 r이 노출되어도 재전송공격은 불가능하다. r은 일회용이므로

정답 : ④

11. 백도어 탐지 방법으로 옳지 않은 것은? [2022년 국회 9급]

① 현재 동작 중인 프로세스 및 열린 포트 확인
② SetUID 파일 검사
③ 백신 등 바이러스 탐지 툴 사용
④ 무결성 검사
⑤ 실행 파일 패킹

♤ **백도어 탐지 방법**

① 현재 동작 중인 프로세스 및 열린 포트 확인 → ps 이용, **모르는 프로세스 실행** 여부 확인
② SetUID 파일 검사 → SetUID 권한 파일 검사(백도어 프로그램이 주로 사용하므로)
③ 백신 등 바이러스 탐지 툴 사용 → 백신 이용, 백도어 프로그램 탐지 가능
④ 무결성 검사 → Tripwire 이용, 파일 무결성 검사
⑤ 실행 파일 패킹(×) → **리버스엔지니어링** 막기 위해 파일 **압축** 또는 **암호화**하는 것**(백도어와 무관)**

백도어	• 백도어 프로그램은 시스템 관리자나 프로그래머가 컴퓨터에 로그인해 들어가는 과정을 쉽게 하려고 **변칙**적으로 개발한 프로그램이다. • 몰래 탑재되어 정상적인 **인증**을 거치지 않고 보안을 해제할 수 있는 **악성코드**이다. • 일반적으로 백도어는 **탐지**되는 것을 **방지**하기 위해서 **찾기 어렵게 설계**된다.

정답 : ⑤

12. 다음에서 설명하는 해킹 공격 방법은? [2018년 컴일 국가 9급]

공격자는 사용자의 합법적 도메인을 탈취하거나 도메인네임시스템(DNS) 또는 프락시 서버의 주소를 변조하여, 사용자가 진짜 사이트로 오인하여 접속하도록 유도한 후 개인정보를 훔친다.

---

① 스니핑(sniffing)　② 파밍(pharming)
③ 트로이 목마(trojan horse)　④ 하이재킹(hijacking)

♤ **파밍(pharming)**

- 파밍은 피싱에서 더 나아간 해킹 기술이다. 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 은행계좌, 신용카드정보, 주민등록번호 같은 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 정상 사이트의 **도메인이름**을 정확히 입력해도 가짜 사이트로 연결되는 해킹 기술이다.
- 파밍은 **정확한 도메인이름을 입력**해도 가짜 웹서버에 접속되어 개인정보가 도용되는 것이다.
- 파밍은 이용자 PC의 호스트(hosts) 파일을 변조하는 악성코드에 감염되어 발생한다.
- 파밍 예방은 hosts 파일에 은행, 공공기관 등의 도메인이 추가되어 있는지 확인하면 된다.
- 파밍은 호스트(hosts) 파일에 은행, 공공기관의 도메인이 추가되어 있는지 확인하면 된다.
- hosts 파일을 메모장 프로그램을 이용해서 열어보면 변조된 것을 확인할 수 있다.
- 파밍은 한국 형법상 개인정보수집 위반죄, 변작죄, 절도죄, 사기죄 등이 성립될 수 있다.

정답 : ②

13. 파밍(pharming) 공격에 활용하기 위해 공격자의 웹서버 IP 주소와 매핑해주는 특정 정보로 옳은 것은? [2018년 국회 9급]

① 정상 사이트의 도메인 주소
② 정상 사이트 서버의 MAC 주소
③ 정상 사이트가 연결되어 있는 스위치의 port 번호
④ 사용자 컴퓨터의 공인 IP주소
⑤ 정상 사이트 서버의 TCP port 번호

♤ **파밍 공격**

- 파밍은 피싱에서 더 나아간 해킹 기술이다. 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 은행계좌, 신용카드정보, 주민등록번호 같은 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 정상 사이트의 **도메인이름**을 정확히 입력해도 가짜 사이트로 연결되는 해킹 기술이다.

정답 : ①

14. 사용자가 웹브라우저에서 정확한 웹페이지 주소를 입력하여도 가짜 웹페이지로 접속되는 피싱 공격은? [2022년 국가 7급]

① 보이스 피싱(voice phishing)
② 메신저 피싱(messenger phishing)
③ 스미싱(smishing)
④ 파밍(pharming)

♤ **파밍**

- 파밍은 피싱에서 더 나아간 해킹 기술이다. 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 은행계좌, 신용카드정보, 주민등록번호 같은 개인정보를 훔치기 위한 사기 기술이다.
- 파밍은 정상 사이트의 **도메인이름**을 정확히 입력해도 가짜 사이트로 연결되는 해킹 기술이다.
- 파밍은 **정확한 도메인이름을 입력**해도 **가짜 웹서버**에 접속되어 개인정보가 도용되는 것이다.
- 파밍은 이용자 PC의 호스트(hosts) 파일을 변조하는 악성코드에 감염되어 발생한다.
- 파밍 예방은 hosts 파일에 은행, 공공기관 등의 도메인이 추가되어 있는지 확인하면 된다.
- 파밍은 호스트(hosts) 파일에 은행, 공공기관의 도메인이 추가되어 있는지 확인하면 된다.
- hosts 파일을 메모장 프로그램을 이용해서 열어보면 변조된 것을 확인할 수 있다.
- 파밍은 한국 형법상 개인정보수집 위반죄, 변작죄, 절도죄, 사기죄 등이 성립될 수 있다.

정답 : ④

15. 다음 중 양자 컴퓨팅과 관련한 설명으로 가장 옳지 않은 것은? [2022년 군무원 7급]

① 양자 컴퓨터에 Shor 알고리즘을 적용하면 현재 알려진 다수의 대칭키 암호화 알고리즘이 다항시간 내에 공격 가능해지므로 안전하지 않게 된다.
② 양자 키 분배(quantum key distribution)에서는 양자 물리학의 중첩과 얽힘의 성질을 이용하여 도청으로부터 안전한 키 분배 방식을 제공한다.
③ 양자내성암호(post-quantum cryptography)는 양자 컴퓨터가 등장하더라도 안전성을 보장하는 암호 알고리즘을 일컬으며, NIST에 의해 후보 알고리즘이 검토되고 있다.
④ 마이크로소프트에서는 양자 알고리즘을 개발하고 실행하기 위한 Q# 오픈소스 프로그래밍 언어를 개발하였다.

♤ **양자 컴퓨팅**

- 양자 컴퓨터에 **Shor 알고리즘**을 적용하면 현재 알려진 다수의 **대칭키** 암호화 알고리즘이 다항시간 내에 공격 가능해지므로 안전하지 않게 된다.**(×)**
  → 쇼어 알고리즘은 **소인수분해**를 빠르게 처리할 수 있는 양자 알고리즘이다.
  → **소인수분해** 해결 시간을 감소시키므로 **공개키 암호(RSA 등)**를 사용할 수 없도록 한다.

정답 : ①

16. 공격자가 해킹을 통해 시스템에 침입하여 루트 권한을 획득한 후, 재침입할 때 권한을 쉽게 획득하기 위하여 제작된 악성 소프트웨어는? [2022년 지방 9급]

① 랜섬웨어 ② 논리폭탄
③ 슬래머 웜 ④ 백도어

♤ **백도어(back door) / 트랩도어(trap door)**

- 백도어와 트랩도어는 프로그램의 일종으로 같은 의미로 사용된다.
- 백도어는 **시스템 보안이 제거된 비밀통로**를 지칭한다.
- 백도어는 시스템 설계자가 고의로 만들어 놓은 시스템의 비밀통로이다.
- 백도어는 유지보수 등을 위한 접근 편의를 위해 만들어 놓은 시스템의 비밀통로이다.
- 프로그램 개발에서 코드 내에 백도어라는 중단 부분을 설정하여 보수할 수 있게 한다.
- 백도어는 최종 단계에서 삭제되어야 한다. 남아 있으면 범죄에 악용되기도 한다.
- 초기에는 백도어는 주로 프로그래머들이 로그인 등 편의를 위해 만들었다.
- 그 후, **해커**들이 **백도어**를 만들어 **공격** 컴퓨터 **침입 수단**으로 사용하고 있다.
- 백도어 프로그램은 시스템 관리자나 프로그래머가 컴퓨터에 로그인해 들어가는 과정을 쉽게 하려고 변칙적으로 개발한 프로그램이다.

예	네트워크상에서 다른 컴퓨터로 접속할 때 단축키('A', 'F9' 등)를 누르면 바로 해당 컴퓨터에 접속할 수 있도록 한 것이다.

정답 : ④