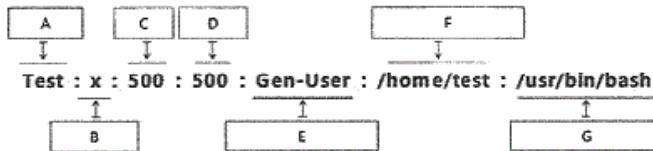


학번		이름	
----	--	----	--

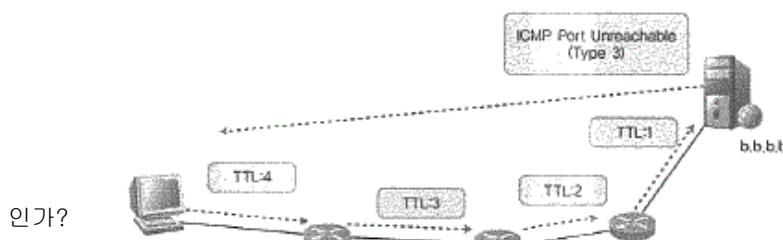
1. 다음은 passwd 파일 구조를 나타내는 그림이다. “G”가 의미하는 것은?



5. 인증 장치에 대한 설명으로 옳은 것은?

- ① USB 메모리에 디지털 증명서를 넣어 인증 디바이스로 하는 경우 그 USB 메모리를 접속하는 PC의 MAC 어드레스가 필요하다.
- ② 성인의 홍채는 변화가 없고 홍채 인증에서는 인증 장치에서의 패턴 갱신이 불필요하다.
- ③ 정전용량 방식의 지문인증 디바이스 LED 조명을 설치한 실내에서는 정상적으로 인증할 수 없게 될 가능성이 높다.
- ④ 인증에 이용되는 접촉형 IC 카드는 카드 내의 코일의 유도 기전력을 이용하고 있다.

17. 다음 그림은 a.a.a.a 시스템에서 UDP 패킷을 TTL=1부터 하나씩 늘려가면서 b.b.b.b로 전송하고, TTL=4일 때 b.b.b.b 시스템에 UDP 패킷이 도달하고 ICMP Port Unreachable(Type 3) 패킷이 a.a.a.a 시스템으로 돌아왔다. 무엇을 하기 위한 과정



- ① ICMP scan
- ② traceroute
- ③ ping
- ④ UDP scan

20. 다음 중 인증의 방법이 아닌 것은?

- ① 당신이 알고 있는 것(Something You Know)
- ② 당신이 위치를 알고 있는 곳(Somewhere You Know)
- ③ 당신이 가지고 있는 것(Something You Have)
- ④ 당신 모습 자체(Something You Are)

30. 다음 중 일반적으로 사용되는 서비스와 해당 서비스의 기본 설정 포트연결이 틀린 것은?

- ① SSH(Secure Shell) – 22
- ② SMTP(Simple Mail Transfer Protocol) – 25
- ③ FTP(File Transfer Protocol) – 28
- ④ HTTPS(Hyper-Text Transfer Protocol over Secure layer) – 443

31. 네트워크 도청을 예방하기 위한 대책으로 틀린 것은?

- ① 업무용 무선 AP와 방문자용 AP를 같이 사용한다.
- ② 무선 AP의 비밀번호는 쉽게 예측하지 못하는 안전한 비밀번호로 설정한다.
- ③ 업무용 단말기는 방문자용 AP에 접속하지 않도록 조치한다.
- ④ 중요 정보는 암호화 통신을 이용하여 전송한다.

36. 다음 문장의 괄호 안에 들어갈 말은?

Anti Sniffer 도구들의 특징은 로컬 네트워크에서 네트워크 카드의 () 면부를 체크하여 스니퍼가 돌고 있는지를 파악한다.

- ① Duplex Mode
- ② MAC
- ③ Promiscuous Mode
- ④ ARP

42. OTP에 대한 설명으로 틀린 것은?

- ① 의미있는 숫자로 구성된다.
- ② 비밀번호 재사용이 불가능하다.
- ③ 비밀번호 유추가 불가능하다.
- ④ 사전 공격(Dictionary Attack)에 안전하다.

43. 웹 어플리케이션 취약성 조치방안에 대한 설명으로 틀린 것은?

- ① server side session 방식은 침해 가능성도 있고, 구조상 다양한 취약점에 노출될 수 있으므로 가볍고 안전한 client side의 cookie를 사용한다.
- ② 모든 인자에 대해 사용 전에 입력값 검증을 수행하도록 구성한다.
- ③ 파일 다운로드시 위치는 지정된 데이터 저장소를 지정하여 사용하고 데이터 저장소 상위로 이동되지 않도록 구성한다.
- ④ SSL/TLS와 같은 기술을 이용하여 로그인 트랙잭션 전체를 암호화한다.

51. 다음 문장의 괄호 안에 알맞은 용어는?

과거 ()공격은 불특성 다수를 대상으로 데이터를 암호화하고 이에 대한 몸값을 요구하는 방식이 대부분이었다. 그러나 최근에는 높은 금액을 지불할 수 있는 대규모 엔터프라이즈 환경이 주로 공격 대상이 되고 있고 암호화 뿐만 아니라 데이터 유출 후 인터넷 공개를 미끼로 협박하는 혈태의 공격 방식으로 진화되고 있다. 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.

62. 접근통제 모델에 대한 각각의 설명 중 옳은 것은?

- ① 비바(Biba) 모델 : 임의적 접근통제(DAC: Discretionary Access Control)를 기반으로 하는 상태 머신 모델이다.
- ② 벨-라파둘라(Bell-Lapadula) 모델 : 객체에 대한 무결성 또는 가용성을 유지하는데 중점을 두고 있으며, 기밀성의 측면에는 대처하지 않는다.
- ③ 비바(Biba) 모델 : 비밀 채널을 방지하며, 내부 및 외부 객체 일관성을 보호한다.
- ④ 클락-윌슨(Clark-Wilson) 모델 : 허가 받은 사용자가 허가 받지 않고 데이터를 수정하는 것을 방지한다.

65. 접근통제정책 구성요소에 대한 설명으로 틀린 것은?

- ① 사용자 : 시스템을 사용하는 주체이다.
- ② 자원 : 사용자가 사용하는 객체이다.
- ③ 행위 : 객체가 행하는 논리적 접근통제이다.
- ④ 관계 : 사용자에게 승인된 허가(읽기, 쓰기, 실행)이다.

2025. 학습정리

61. 다음 지문에서 설명하는 정보보호 용어는?

조직이나 시스템에 손실 또는 손해를 유발시킬 수 있는 사항들의 집합으로 정의된다. 예로는 해킹, 악성코드, 파손 행위, 화재 등을 들 수 있다.

- ① 위협(threat)
- ② 취약점(vulnerability)
- ③ 자산(asset)
- ④ 위험(risk)

62. 다음 지문에서 설명하고 있는 원칙은?

- 개발자는 운영 데이터에 접근할 수 없으나 테스트를 위해 관리자의 승인을 받을 경우 제한된 규모의 운영 데이터에 접근할 수 있다.
- 서버 관리자는 시스템 로그에 접근할 수 없다.

- ① 직무 순환
- ② 상호 배제
- ③ 책임추적성 보장
- ④ 직무 분리

69. 다음 지문에서 설명하는 접근통제 모델은?

이 모델은 객체에 대한 소유권을 기반으로 소유권을 갖는 주체가 객체에 대한 권한의 일부 또는 전부를 다른 주체에게 부여할 수 있다.

- ① 강제적 접근통제 모델
- ② 규칙기반 접근통제 모델
- ③ 역할기반 접근통제 모델
- ④ 임의적 접근통제 모델

71. 다음 중 역할기반 접근통제(Role Based Access Control)의 설명으로 틀린 것은?

- ① 대개 구현을 위하여 역할에 대한 추상화 작업이 요구된다.
- ② Non-DAC 또는 비임의적 접근통제 모델로도 불린다.
- ③ 사용자의 역할 및 직능에 따라 접근을 통제하는 방식이다.
- ④ 사용자에게 지나친 권한이 부여될 우려가 있다.

82. 개인정보의 안정성 확보조치 기준(고시)의 제7조(개인정보의 암호화)에 따라 반드시 암호화하여 저장해야하는 개인정보가 아닌 것은?

- ① 비밀번호
- ② 고유식별번호
- ③ 바이오 정보
- ④ 전화번호

84. 정보보호 내부 감사 시 고려해야 할 사항으로 가장 부적합한 것은?

- ① 내부감사를 수행하는 구성원은 정보보호 전문가들로 제한한다.
- ② 감사의 범위는 다양한 위험을 분석 및 검토할 수 있도록 가능한 포괄적이어야 한다.
- ③ 감사활동은 기업 내외부로부터 독립성을 유지할 수 있도록 해야 한다.
- ④ 내부감사는 조직의 위험을 파악하여 개선사항을 제시할 수 있다.

85. 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업의 내부관리계획의 내용에 포함하지 않아도 될 사항은 무엇인가?

- ① 개인정보 보호책임자의 지정에 관한 사항
- ② 개인정보 유출사고 대응 · 계획 수립 · 시행에 관한 사항
- ③ 개인정보의 암호화 조치에 관한 사항

- ④ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

87. 개인정보처리자가 정보주체의 동의를 받을 때 정보주체에게 알려야 하는 항목이 아닌 것은?

- ① 개인정보의 수집 · 이용 목적
- ② 수집하려는 개인정보의 항목
- ③ 개인정보의 보유 및 이용 기간
- ④ 개인정보의 수집 출처