1과목 : 정보보호개론

1. Kerberos의 용어 설명 중 옳지 않은 것은?
   ① AS : Authentication Server
   ② KDC : Kerberos 인증을 담당하는 데이터 센터
   ③ TGT : Ticket을 인증하기 위해서 이용되는 Ticket
   ④ Ticket : 인증을 증명하는 키

2. 금융기관이나 인터넷 상에서 많은 사람들로부터 적은 금액을 조금씩 빼내고 피해자는 사건이 알려지기 전까지 전혀 눈치 채지 못하는 컴퓨터 사기수법은?
   ① Scavenging
   ② 논리 폭탄(Logic Bomb)
   ③ 살라미(Salami) 기법
   ④ 자료의 부정변개(Data Diddling)

3. 공개키 암호 알고리즘에 관한 설명 중 옳지 않은 것은?
   ① 공개키 암호화 방식은 암호화와 복호화하는데 비밀키와 공개키라는 서로 다른 두 개의 키를 사용한다.
   ② 공개키는 일반인에게 공개하고 비밀키는 오직 자신만이 알도록 한다.
   ③ 데이터 암호화 및 수신된 데이터의 부인 봉쇄 그리고 전자 서명에 있어서 효율적이다.
   ④ 비공개키 암호 알고리즘보다 암호화와 복호화 속도가 빠르고 키의 길이가 대칭키 알고리즘보다 작다.

4. 다음 내용은 무엇을 설명하는 것인가?

- 데이터 전송 도중이나 DB에 저장되어 있는 정보가 악의의 목적으로 위조 또는 변조되는 것을 방지하는 것이다.

   ① 기밀성(Confidentiality)
   ② 무결성(Integrity)
   ③ 인증(Authentication)
   ④ 부인 방지(Non-Repudiation)

5. SEED(128 비트 블록 암호 알고리즘)의 특성으로 옳지 않은 것은?
   ① 데이터 처리단위는 8, 16, 32 비트 모두 가능하다.
   ② 암・복호화 방식은 공개키 암호화 방식이다.
   ③ 입출력의 크기는 128 비트이다.
   ④ 라운드의 수는 16 라운드이다.

6. SET(Secure Electronic Transaction)의 기술구조에 대한 설명으로 옳지 않은 것은?
   ① SET은 기본적으로 X.509 전자증명서에 기술적인 기반을 두고 있다.
   ② SET에서 제공하는 인터넷에서의 안전성은 모두 암호화에 기반을 두고 있고, 이 암호화 기술은 제 3자가 해독하기가 거의 불가능하다.
   ③ 암호화 알고리즘에는 공개키 암호 시스템만 사용된다.
   ④ 이 방식은 n명이 인터넷상에서 서로 비밀통신을 할 경우 ´n(n-1)/2´ 개 키를 안전하게 관리해야 하는 문제점이 있다.

7. 다음 내용은 보안 운영체제의 특정한 보안기능에 대해 설명한 것이다. 어떤 기능인가?

- 일반적으로 보안 관련 사건 기록의 유지를 포함하며 발생한 각각의 사건과 관련된 사용자의 정보가 수록된다. 모든 보안 관련 사건은 반드시 이 기록부(log file)에 기록되어야 한다. 또한 이 기록부는 명백하게 보호 되어야 한다.

   ① 사용자 식별 또는 인증
   ② 감사 및 감사 기록
   ③ 강제적/임의적 접근 통제
   ④ 침입탐지

8. 안전한 Linux Server를 구축하기 위한 방법으로 옳지 않은 것은?
   ① 불필요한 데몬을 제거한다.
   ② 불필요한 Setuid 프로그램을 제거한다.
   ③ 시스템의 무결성을 주기적으로 검사한다.
   ④ 무결성을 검사하기 위한 데이터베이스를 추후 액세스가 용이하게 검사할 시스템에 저장하는 것이 좋다.

9. 공개키 인증서에 대한 설명 중 옳지 않은 것은?
   ① 공개키 인증서는 주체의 이름과 공개키를 암호학적으로 연결하여, 주체의 공개키에 대한 무결성과 인증성을 제공하기 위한 데이터 구조이다.
   ② 공개키 인증서를 관리하는 체계가 공개키 기반구조(PKI : Public-Key Infrastructure)이다.
   ③ 공개키 인증서의 주요 필드는 일련번호, 주체 이름, 주체 공개키, 발행자 이름, 발행자 서명 알고리즘 등을 포함한다.
   ④ 공개키 인증서는 한번 발급되고 나면 유효기간 동안에 계속 사용되어야 한다.

10. IPSec을 위한 보안 연계(Security Association)가 포함하는 파라미터로 옳지 않은 것은?
    ① IPSec 프로토콜 모드(터널, 트랜스포트)
    ② 인증 알고리즘, 인증키, 수명 등의 AH 관련 정보
    ③ 암호 알고리즘, 암호키, 수명 등의 ESP 관련 정보
    ④ 발신지 IP Address와 목적지 IP Address

2과목 : 운영체제

11. Linux에서 프로세스 실행 우선순위를 바꿀 수 있는 명령어는?
    ① chps ② reserv
    ③ nice ④ top

12. Linux에서 현재 사용하고 있는 쉘(Shell)을 확인해 보기 위한 명령어는?
    ① echo $SHELL ② vi $SHELL
    ③ echo &SHELL ④ vi &SHELL

13. 다음 중 ´/proc´에 관한 설명으로 거리가 먼 것은?
    ① 하드디스크 상에 적은 양의 물리적인 용량을 갖고 있다.
    ② 만약 파일 시스템 정보를 보고자 한다면 ´cat

/proc/filesystems´ 명령을 실행하면 된다.

③ 이 디렉터리에 존재하는 파일들은 커널에 의해서 메모리에 저장된다.

④ 이 디렉터리에는 시스템의 각종 프로세서, 프로그램정보 그리고 하드웨어 적인 정보들이 저장된다.

14. Linux 시스템 명령어 중 디스크의 용량을 확인하는 명령어는?

① cd ② df

③ cp ④ mount

15. Linux 파일 시스템의 기본 구조 중 파일에 관한 중요한 정보를 싣는 곳은?

① 부트 블록 ② i-node 테이블

③ 슈퍼 블록 ④ 실린더 그룹 블록

16. 다음 명령어 중에서 시스템의 메모리 상태를 보여주는 명령어는?

① mkfs ② free

③ ps ④ shutdown

17. Linux의 기본 명령어 ´man´의 의미는?

① 명령어에 대한 사용법을 알고 싶을 때 사용하는 명령어

② 윈도우나 쉘을 빠져 나올 때 사용하는 명령어

③ 지정한 명령어가 어디에 있는지 경로를 표시

④ 기억된 명령어를 불러내는 명령어

18. Windows Server의 DNS 서비스 설정에 관한 설명으로 옳지 않은 것은?

① 정방향 조회 영역 설정 후 반드시 역방향 조회 영역을 설정해 주어야 한다.

② Windows Server는 고정 IP Address를 가져야 한다.

③ Administrator 권한으로 설정해야 한다.

④ 책임자 이메일 주소의 at(@)은 마침표(.)로 대체된다.

19. Linux의 Fdisk 명령어에서 Disk의 명령어 리스트를 보여주는 옵션은?

① m ② d

③ n ④ t

20. 아파치 웹서버는 ´access.conf´를 사용하여 외부접근 제어를 한다. 각 설정에 대한 설명으로 옳지 않은 것은?

① order deny, allow
allow from linux1.nycom.net
deny from all
=》 linux1.nycom.net부터의 연결 요구만을 허락한다.

② order deny, allow
allow from linux1.mydom.net linux2.mydom.net linux3.mydom.net
deny from all
=》 linux1.mydom.net, linux2.mydom.net, linux3.mydom.net부터의 연결 요구만을 허락한다.

③ order deny, allow
allow from all
deny from hackers.annoying.net
=》 hackers.annoying.net부터의 연결 요구만을 거절한다.

④ order mutual-failure
allow from foobirds.org
deny from linux1.foobirds.org linux2.foobirds.org
=》 foobirds.org에 있는 모든 호스트로부터의 연결 요구만을 허락한다.

21. Linux 시스템의 shadow 파일 내용에 대한 설명으로 올바른 것은?

```
Root:$1$szfVKcHi$dEFUonrDJZ2ZGOPuqq9yK0:11458:0:99999:7:::
adm:*:11458:0:99999:7:::
lp:*:11458:0:99999:7:::
named:!!:11458:0:99999:7:::
gdm:!!:11458:0:99999:7:::
```

① lp에서 ´*´은 로그인 쉘을 갖고 있으며, 시스템에 누구나 로그인할 수 있음을 의미한다.

② gdm에서 ´!!´은 로그인 쉘을 갖고 있지만 누구도 계정을 통해서 로그인할 수 없도록 계정이 잠금 상태라는 것을 의미한다.

③ 로그인 계정이 아닌 시스템 계정은 named와 gdm 이다.

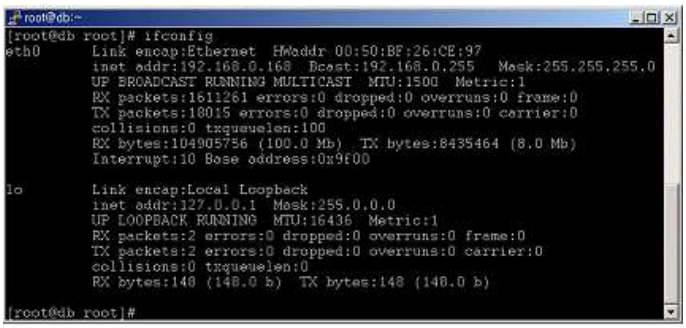
④ root의 암호는 11458 이다

22. Windows Server에서 감사정책을 설정하고 기록을 남길 수 있는 그룹은?

① Administrators ② Security Operators

③ Backup Operators ④ Audit Operators

23. 아래는 Linux 시스템의 ifconfig 실행 결과이다. 옳지 않은 것은?



① eth0의 OUI 코드는 26:CE:97 이다.

② IP Address는 192.168.0.168 이다.

③ eth0가 활성화된 후 현재까지 충돌된 패킷이 없다.

④ lo는 Loopback 주소를 의미한다.

24. Linux 시스템이 부팅될 때 나오는 메시지가 저장된 로그 파일의 경로와 명칭으로 올바른 것은?

① /var/log/boot ② /var/log/dmesg

③ /var/log/message ④ /var/log/secure

25. 아래는 DNS Zone 파일의 SOA 레코드 내용이다. SOA 레코드의 내용을 보면 5 개의 숫자 값을 갖는데, 그 중 두 번째 값인 Refresh 값의 역할은?

```
@ IN SOA localhost. root.localhost.(
        1997022700 ; Serial
        28800      ; Refresh
        14400      ; Retry
        3600000    ; Expire
        86400 )    ; Minimum
```

① Primary 서버와 Secondary 서버가 동기화 하게 되는 기간이다.

② Zone 내용이 다른 DNS 서버의 Cache 안에서 살아남을 기간이다.

③ Zone 내용이 다른 DNS 서버 안에서 Refresh 될 기간이다.

④ Zone 내용이 Zone 파일을 갖고 있는 서버 내에서 자동 Refresh 되는 기간이다.

26. VI(Visual Interface) 에디터에서 편집행의 줄번호를 출력해 주는 명령은?

① :set nobu ② :set nu

③ :set nonu ④ :set showno

27. Linux 시스템을 곧바로 재시작 하는 명령으로 옳지 않은 것은?

① shutdown -r now ② shutdown -r 0

③ halt ④ reboot

28. 다음의 에러를 복구하기 위해서 VI 에디터를 실행시킬 때 가장 적합한 옵션은?

> - Telnet을 이용해서 원격으로 서버에 있는 'a.txt' 파일을 VI 에디터로 편집하던 중 갑자기 접속이 끊어졌다. 다시 접속하여 'a.txt' 파일을 열었더니, 'a.txt' 파일이 열리기 전에 한 페이지 가량의 에러 메시지가 출력된 후 Enter 키를 눌러야만 'a.txt' 파일이 열린다.

① vi a.txt ② vi -recover a.txt

③ vi -continue a.txt ④ vi -r a.txt

29. Linux에서 'netstat -an' 명령으로 시스템을 확인한 결과 다음과 같은 결과가 나왔다. 아래 '3306'번 포트는 어떤 데몬이 가동될 때 열리는 포트인가? (단, 시스템의 기본 포트는 Well-Known 포트를 사용한다.)

```
[icqa@icqalocal ~]$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22222               0.0.0.0:*                   LISTEN
tcp        0      0 192.168.10.7 :222            3.23 .11 .11 :309          SYN_RECV
tcp        0      0 192.168.10.7 :222            3.23 .11 .11 :348          SYN_RECV
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0     64 192.168.10.7 :222           192.168.10.10 :104          ESTABLISHED
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 ::1:25                      :::*                        LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     10430  private/virtual
unix  2      [ ACC ]     STREAM     LISTENING     10434  private/lmtp
```

① MySQL ② DHCP

③ Samba ④ Backdoor

30. 아파치 데몬으로 웹서버를 운영하고자 할 때 반드시 선택해야하는 데몬은?

① httpd ② dhcpd

③ webd ④ mysqld

3과목 : 네트워크

31. TCP와 UDP의 차이점을 설명한 것 중 옳지 않은 것은?

① TCP는 전달된 패킷에 대한 수신측의 인증이 필요하지만 UDP는 필요하지 않다.

② TCP는 대용량의 데이터나 중요한 데이터 전송에 이용되지만 UDP는 단순한 메시지 전달에 주로 사용된다.

③ UDP는 네트워크가 혼잡하거나 라우팅이 복잡할 경우에는 패킷이 유실될 우려가 있다.

④ UDP는 데이터 전송 전에 반드시 송수신 간의 세션이 먼저 수립되어야 한다.

32. 네트워크 주소 중 B Class 기반의 IP Address로 옳지 않은 것은?

① 139.39.60.101 ② 203.34.1.12

③ 187.124.70.87 ④ 155.98.200.100

33. IPv4에 비하여 IPv6이 개선된 설명으로 잘못된 것은?

① 128bit 구조를 가지기 때문에 기존의 IPv4 보다 더 많은 노드를 가질 수 있다.

② 전역방송(Broad Cast)이 가능하다.

③ IPv6에서는 확장이 자유로운 가변길이 변수로 이루어진 옵션 필드 부분 때문에 융통성이 발휘된다.

④ IPv6에서는 Loose Routing과 Strict Routing의 두 가지 옵션을 가지고 있다.

34. 다음과 같은 일을 수행하는 프로토콜은?

> - 인터넷에 접속한 호스트들은 인터넷 주소에 의해서 식별되지만 실질적인 통신은 물리적인 네트워크 주소를 얻어야 가능하다.

① DHCP(Dynamic Host Configuration Protocol)

② IP(Internet Protocol)

③ RIP(Routing Information Protocol)

④ ARP(Address Resolution Protocol)

35. TCP 헤더 필드의 내용으로 옳지 않은 것은?

① TTL(Time To Live) ② 발신지 포트번호

③ 윈도우 크기 ④ Checksum

36. 네트워크 관리자나 라우터가 IP 프로토콜의 동작 여부를 점검하고, 호스트로의 도달 가능성을 검사하기 위한 ICMP 메시지 종류는?

① Parameter Problem

② Timestamp Request/Response

③ Echo Request/Response

④ Destination Unreachable

37. OSI 7 Layer 중 응용 계층간의 정보 표현 방법의 상이를 극복하기 위한 계층으로, 보안을 위한 암호화/복호화 방법과 효율적인 전송을 위한 압축 기능이 들어 있는 계층은?

① 데이터 링크 계층 ② 세션 계층

③ 네트워크 계층 ④ 표현 계층

38. 아래 내용에 해당하는 서브넷 마스크 값은?

203.76.25.1/26

① 255.255.255.192 ② 255.255.255.224
③ 255.255.255.254 ④ 255.255.255.0

39. 통신 에러제어는 수신측이 에러를 탐지하여 송신자에게 재전송을 요구하는 ARQ(Automatic Repeat Request)를 이용하게 된다. ARQ 전략으로 옳지 않은 것은?

① Windowed Wait and Back ARQ
② Stop and Wait ARQ
③ Go Back N ARQ
④ Selective Repeat ARQ

40. 각 허브에 연결된 노드가 세그먼트와 같은 효과를 갖도록 해주는 장비로서 트리 구조로 연결된 각 노드가 동시에 데이터를 전송할 수 있게 해주며, 규정된 네트워크 속도를 공유하지 않고 각 노드에게 규정 속도를 보장해 줄 수 있는 네트워크 장비는?

① Switching Hub ② Router
③ Brouter ④ Gateway

41. 서브넷 마스크에 대한 설명으로 올바른 것은?

① DNS 데이터베이스를 관리하고 IP Address를 DNS의 이름과 연결한다.
② IP Address에 대한 네트워크를 분류 또는 구분한다.
③ TCP/IP의 자동설정에 사용되는 프로토콜로서 정적, 동적 IP Address를 지정하고 관리한다.
④ 서로 다른 네트워크를 연결할 때 네트워크 사이를 연결하는 장치이다.

42. 네트워크 전송매체에 대한 설명으로 옳지 않은 것은?

① UTP - 쉴딩(Shielding) 처리를 하지 않고 내부의 선이 꼬여 있는 형태이다.
② STP - UTP와 달리 내부의 8개 선에 피복이 입혀져 있지 않다.
③ Thinnet BNC - BNC라는 커넥터가 씬넷(Thinnet) 케이블에 연결되어 있는 형태로 보통 씬넷 케이블 또는 BNC 케이블이라고 부른다.
④ Optical Fiber - 케이블 중앙에 유리섬유 코어나 플라스틱 코어가 있고 맨 바깥에 플라스틱 피복이 입혀져 있다.

43. IPv4 Address에 관한 설명 중 옳지 않은 것은?

① IP Address는 32bit 구조를 가지고 A, B, C, D 네 종류의 Class로 구분한다.
② 127.0.0.1은 루프 백 테스트를 위한 IP Address라고 할 수 있다.
③ B Class는 중간 규모의 네트워크를 위한 주소 Class로 네트워크 ID는 128~191 사이의 숫자로 시작한다.
④ D Class는 멀티캐스트용으로 사용된다.

44. 패킷(Packet)에 있는 정보로 옳지 않은 것은?

① 출발지 IP Address ② TCP 프로토콜 종류
③ 전송 데이터 ④ 목적지 IP Address

45. 디지털 데이터를 디지털 신호 인코딩(Digital Signal Encoding)하는 방법으로 옳지 않은 것은?

① NRZ(Non Return to Zero)
② Manchester
③ PCM(Pulse Code Modulation)
④ Differential Manchester

4과목 : 보안

46. DoS(Denial of Service) 공격과 관련 없는 내용은?

① 관리자 권한을 획득하여 데이터를 파괴할 수 있다.
② 한 예로 TearDrop 공격이 있다.
③ 주로 TCP/IP 프로토콜의 취약성을 이용한다.
④ 공격의 원인이나 공격자를 추적하기 힘들다.

47. 다음에서 설명하는 기법은?

- 인터넷 프로토콜인 TCP/IP의 구조적 결함, 즉 TCP 시퀀스번호, 소스라우팅, 소스 주소를 이용한 인증(Authentication) 메커니즘 등을 이용한 방법으로써, 인증(Authentication) 기능을 가지고 있는 시스템을 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법이다.

① IP Sniffing ② IP Spoofing
③ Race Condition ④ Packet Filtering

48. 침입차단시스템에 대한 설명 중 옳지 않은 것은?

① 침입차단시스템은 내부 사설망을 외부의 인터넷으로부터 보호하기 위한 장치이다.
② 패킷 필터링 침입차단시스템은 주로 발신지와 목적지 IP Address와 발신지와 목적지 포트 번호를 바탕으로 IP 패킷을 필터링한다.
③ 침입차단시스템의 유형은 패킷 필터링 라우터, 응용 레벨 게이트웨이, 그리고 회선 레벨 게이트웨이 방법 등이 있다.
④ 침입차단시스템은 네트워크 사용에 대한 로깅과 통계자료를 제공할 수 없다.

49. 다음은 어떤 보안 도구를 의미하는가?

- 회사의 사설 네트워크와 외부의 공중 네트워크 사이의 중립 지역으로서 삽입된 컴퓨터 호스트 또는 소형 네트워크를 말한다.

① IDS ② DMZ
③ Firewall ④ VPN

50. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?

① 안전하지 못한 네트워크에서 안전하게 통신할 수 있는 기능과 강력한 인증방법을 제공한다.
② 문자를 암호화하여 IP Spoofing, DNS Spoofing으로부터 보호할 수 있다.
③ 쌍방 간 인증을 위해 Skipjack 알고리즘이 이용된다.
④ 네트워크의 외부 컴퓨터에 로그인 할 수 있고 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 프로그램이다.

51. 지정된 버퍼보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 하는 해킹 방법은?

① DoS ② Trojan Horse
③ Worm Virus Backdoor ④ Buffer Overflow

52. SSL(Secure Socket Layer)에서 제공되는 정보보호 서비스로 옳지 않은 것은?

① 두 응용간의 기밀성 서비스
② 클라이언트와 서버간의 상호 인증 서비스
③ 교환되는 메시지의 무결성 서비스
④ 상거래에 응용하기 위한 부인 방지서비스

53. Windows Server에서 유지하는 중요 로그 유형에 해당하지 않은 것은?

① Firewall Log ② Security Log
③ System Log ④ Application Log

54. Linux에서 Nmap의 옵션 중 상대방의 OS를 알아내는 옵션은?

① [root@icqa bin]#./nmap -O www.target.com
② [root@icqa bin]#./nmap -I www.target.com
③ [root@icqa bin]#./nmap -sS www.target.com
④ [root@icqa bin]#./nmap -sP www.target.com

55. 현재 Linux 시스템 상에서 침입자의 침입여부나 사용자의 사용여부를 확인하고자 한다. 적합한 명령어로 옳지 않은 것은?

① [root@icqa /bin]#w
② [root@icqa /bin]#netstat -t
③ [root@icqa /bin]#nuser -a
④ [root@icqa /bin]#who

56. 아래와 같이 초기설정이 되어있는 '/bin/su' 명령어가 있다. Linux 서버의 내부 보안을 위해 '/bin/su' 명령어를 root에게는 모든 권한을 'wheel'이라는 그룹에게는 실행권한만을 부여하려고 한다. 이 과정 중에 올바르지 않은 사항은?

```
[rpoot@icqa/bin]# ls -alF su
-rwsr-xr-x 1 root root 14188 3월 7 2017 su*
```

① [root@icqa /bin]#chmod 4710 /bin/su
② [root@icqa /bin]#chown root /bin/su
③ [root@icqa /bin]#chgrp wheel /bin/su
④ [root@icqa /bin]#chown -u root -g wheel /bin/su

57. PGP(Pretty Good Privacy)에서 사용되는 알고리즘이 아닌 것은?

① RSA ② DES
③ MD5 ④ IDEA

58. Linux에서 root 권한 계정이 'a' 라는 파일을 지우려 했을 때 나타난 결과이다. 이 파일을 지울 수 있는 방법은?

```
root@linux /root]# rm -rf a
rm: cannot unlink 'a': Operation not permitted
[root@linux /root]# ls -l a
-rw-r--r-- 1 root root 0 Aug 31 16:59 a
[root@linux4u /root]
```

① 파일크기가 '0' 바이트이기 때문에 지워지지 않으므로, 파일에 내용을 넣은 후 지운다.
② 현재 로그인 한 사람이 root가 아니므로 root로 로그인한다.
③ chmod 명령으로 쓰기금지를 해제한다.
④ chattr 명령으로 쓰기금지를 해제한다.

59. 다음은 어떤 시스템의 messages 로그파일의 일부이다. 로그파일의 분석으로 옳지 않은 것은?

```
Aug 27 04:02:01 linux syslogd 1.3-3: restart.
Aug 28 19:15:29 linux login: FAILED LOGIN 1 FROM 211.39.62.2 FOR , User not known to the
  underlying authentication module
Aug 28 19:15:35 linux PAM_pwdb[19186]: (login) session opened for user gozila by (uid=0)
Aug 28 19:15:50 linux rz[19200]: [gozila] firewall.txt/ZMODEM: 5358 Bytes, 3491 BPS
Aug 28 20:11:02 linux PAM_pwdb[19280]: authentication failure; bomb(uid=500) -> root for su service
Aug 28 20:11:14 linux PAM_pwdb[19282]: (su) session opened for user root by batman(uid=500)
Aug 28 20:43:10 linux PAM_pwdb[19282]: (su) session closed for user root
Aug 29 15:56:10 linux PAM_pwdb[20642]: check pass; user unknown
Aug 29 15:56:11 linux login[20642]: FAILED LOGIN 1 FROM s210-219-171-189.thrunet.ne.kr FOR guest,
  User not known to the underlying authentication module
```

① 8월 27일 syslog daemon이 재구동된 적이 있다.
② 8월 28일 gozila라는 ID로 누군가 접속한 적이 있다.
③ 8월 28일 gozila라는 ID로 누군가가 접속하여 firewall.txt 파일을 다운 받아갔다.
④ batman 이라는 사람이 8월 28일에 su 명령을 사용하여 root 권한을 얻었다.

60. 스머프 공격(Smurf Attack)에 대한 설명으로 올바른 것은?

① 두 개의 IP 프래그먼트를 하나의 데이터 그램인 것처럼 하여 공격 대상의 컴퓨터에 보내면, 대상 컴퓨터가 받은 두 개의 프래그먼트를 하나의 데이터 그램으로 합치는 과정에서 혼란에 빠지게 만드는 공격이다.
② 서버의 버그가 있는 특정 서비스의 접근 포트로 대량의 문자를 입력하여 전송하면, 서버의 수신 버퍼가 넘쳐서 서버가 혼란에 빠지게 만드는 공격이다.
③ 서버의 SMTP 서비스 포트로 대량의 메일을 한꺼번에 보내고, 서버가 그것을 처리하지 못하게 만들어 시스템을 혼란에 빠지게 하는 공격이다.
④ 출발지 주소를 공격하고자 하는 컴퓨터의 IP Address로 지정한 후, 패킷신호를 네트워크 상의 컴퓨터에 보내게 되면, 패킷을 받은 컴퓨터들이 반송 패킷을 다시 보내게 되는데, 이러한 원리를 이용하여 대상 컴퓨터에 갑자기 많은 양의 패킷을 처리하게 함으로써 시스템을 혼란에 빠지게 하는 공격이다.

1	2	3	4	5	6	7	8	9	10
②	③	④	①	②	③	②	④	④	④
11	12	13	14	15	16	17	18	19	20
③	①	①	②	②	②	①	①	①	④
21	22	23	24	25	26	27	28	29	30
②	①	①	②	①	②	③	④	①	①
31	32	33	34	35	36	37	38	39	40
④	②	②	④	①	③	④	①	①	①
41	42	43	44	45	46	47	48	49	50
②	②	①	②	③	①	②	④	②	③
51	52	53	54	55	56	57	58	59	60
④	④	①	①	③	④	②	④	③	④