2001년02월25일년 인터넷보안전문가 2급 필기시험 기출문제 답안

【1과목 : 10문제】 정보보호개론	1	2	3	4	5	6	7	8	9	10
	④	③	①	①	④	③	④	④	④	②

【2과목 : 20문제】 운영체제	11	12	13	14	15	16	17	18	19	20
	③	③	②	①	③	①	③	④	④	②
	21	22	23	24	25	26	27	28	29	30
	④	①	③	②	①	③	②	①	①	②

【3과목 : 15문제】 네트워크	31	32	33	34	35	36	37	38	39	40
	③	②	②	③	①	③	④	③	②	①
	41	42	43	44	45					
	④	④	①	③	④					

【4과목 : 15문제】 보안	46	47	48	49	50	51	52	53	54	55
	④	③	①	④	③	②	②	④	①	①
	56	57	58	59	60					
	④	③	④	②	④					

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.

CBT기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 정보보호개론 (10문제)

1. PES 암호화 알고리즘에서 발전하였으며, 블록알고리즘으로 64 비트 평문에서 동작하며 키의 길이는 128bit, 8 라운드의 암호화 방식을 지원하는 암호 알고리즘은?

① DES
② Skipjack
③ MISTY
❹ IDEA

2. 다음 중 암호화 알고리즘 성격이 다른 하나는?.

① DES
② Skipjack
❸ RSA
④ FEAL

3. 다음은 사용자 인증시 기본적으로 지켜져야 할 보안원칙들이다. 이중 Redhat linux 6.2 버전의 기본 console login 때 적용되지 않는 보안원칙은? (일반유저가 로그인했을때를 기준으로 한다.)

❶ 잘못된 암호가 정해진 회수만큼 입력되면 해당사용자의 ID 는 일정시간동안 로그인이 불가능해진다.
② 패스워드는 내부적으로 암호화하여 저장한다.
③ 패스워드 구문은 최소 6 자 이상이어야 한다.
④ 패스워드 변경시 이전 패스워드가 재사용 되어서는 안된다.

4. 전화접속으로 시스템에 접근할 경우 우선 사용자의 신분을 확인한 후, 시스템이 접속을 단절한 후 사전에 등록된 해당 사용자의 전화번호로 재접속하여 다른 사용자가 승인된 사용자 인 것을 가장하여 전화접속으로 시스템에 접근하는 것을 막는 보안 서비스가 Windows NT 4.0 에 구현되어있다. 이 서비스(기능)의 명칭은?

❶ RAS Callback
② WINS
③ kerberos
④ LDAP

5. 다음 중 컴퓨터바이러스 감염을 방지하기 위한 기술적인 예방대책과 거리가 먼 것은?

① 주기적으로 여러 개의 바이러스진단 프로그램을 이용하여 하드디스크를 검사한다.
② 부팅시 바이러스를 점검하는 메모리 상주프로그램이 자동 실행될 수 있도록 한다.
③ 실행파일은 읽기전용으로 파일속성을 변경한다.
❹ 매시간 정기적인 백업을 한다.

6. 국내 침입차단 시스템 평가기준에 대한 설명 중 옳지 않은 것은?

① K0 : 평가신청인이 신청한 침입차단 시스템의 평가결과가 등급별 요구사항을 만족하지 못함을 의미한다.
② K2 : 보안행위에 대한 감사기록을 생성, 관리할 수 있어야 하며, 비정형화된 기본설계를 요구한다.
❸ K3 : 강제적 접근통제와 보안레이블과 같은 부가적인 보안 서비스를 이용한 침입차단시스템의 접근통제 강화가 요구된다.
④ K6 : K5 등급의 요구조건을 만족함과 동시에 외부침입자의 불법침입 행위를 감지할 수 있는 기능을 제공하여야 한다.

7. 다음 중 침입차단 시스템의 문제점으로 볼 수 없는 것은?

① 제한된 서비스
② 내부 사용자에 의한 보안 침해
③ 침입차단 시스템의 네트워크 트레픽 병목발생
❹ 보안기능의 집중화

8. 다음 정보보안과 관련된 행위 중 법률적으로 처벌할 수 없는 행위는?

① 남의 컴퓨터의 공유자원을 열어서 업무와 관련된 자료를 삭제한 행위
② 정부기관의 DB 자료를 임의로 수정한 행위
③ 경품응모행사중인 회사의 웹서버 프로그램의 허점을 이용 경품응모 당첨확률을 높인 행위
❹ 컴퓨터 바이러스를 제작하여 소스를 공개한 행위

9. 다음 중 전자상거래와 관련하여 설명이 잘못된 것은?

① 전자상거래에서 전자지불시스템은 신용카드, 전자화폐, 전자수표 및 전자자금이체 기반으로 분류할 수 있다.

② SET(Secure Electronic Transaction) 프로토콜은 상점등록, 고객등록, 구매요구 프로토콜 등이 주된 내용이다.

③ 전자상거래의 보안요구 사항은 무결성, 비밀성, 인증, 권한부여 등이다.

❹ 전자상거래의 보안구조는 컴퓨터 보안, 네트워크 보안, 인터넷 보안 등으로 분류할 수 있으며, 인터넷 보안의 주요요소는 접근 및 인원 통제이다.

10. 개인 홈페이지 서버가 해킹을 당하여 모든 자료가 삭제되었을 때 취해야할 행동으로 가장 적절한 것은?

① 로그분석을 통해 해킹을 한사람의 신원을 밝혀내 보복한다.

❷ 로그분석을 통해 해킹을 한 시점과 방법을 알아내 차후 동일수법에 의한 사고를 방지한다.

③ 백업된 자료를 이용하여 그대로 복구하여 놓는다.

④ 백도어의 염려가 있으므로 시스템을 포맷한 후 재설치하고, 경찰에 신고한다.

【2과목】 운영체제 (20문제)

11. 다음 중 은폐형 바이러스로 기억장소에 존재하며 마치 감염되지 않은 것처럼 백신 프로그램을 속이게끔 설계된 바이러스의 형태는 몇 세대 바이러스 인가?

① 1세대

② 2세대

❸ 3세대

④ 4세대

12. 파일이 생성된 시간을 변경하기 위해 사용하는 리눅스 명령은?

① chmod

② chgrp

❸ touch

④ chown

13. 파일 퍼미션이 현재 664인 파일이 /etc/file1.txt 라는 이름으로 저장되어있다. 이 파일을 batman이라는 사용자의 홈디렉토리에서 ln 명령을 이용하여 a.txt라는 이름으로 심볼릭 링크를 생성하였는데, 이 a.txt 파일의 퍼미션 설정상태는?

① 664

❷ 777

③ 775

④ 700

14. 시스템에 Apache Web Server의 RPM버전을 구해서 설치하려고 한다. 하지만 Apache를 설치하려고 하는 Linux Server에 이미 RPM버전의 Apache Web Sever가 설치되어 있는지 확인하지 못하였다. 이 경우 기존 Apache가 설치되어있더라도 안전업그레이드 할 수 있는 옵션은?

❶ -U

② -u

③ -i

④ -l

15. 리눅스 콘솔상에서 네트워크어댑터 eth0를 192.168. 1.1이라는 주소로 사용하고 싶을 때 올바른 명령은?

① ifconfig eth0 192.168.1.1 activate

② ifconfig eth0 192.168.1.1 deactivate

❸ ifconfig eth0 192.168.1.1 up

④ ifconfig eth0 192.168.1.1 down

16. 리눅스의 네트워크 서비스에 관련된 설정을 하는 설정파일은?

❶ /etc/inetd.conf

② /etc/fstab

③ /etc/ld.so.conf

④ /etc/profile

17. 리눅스 커널 2.2.부터는 smurf 공격 방지를 위해 icmp 브로드캐스트 기능을 막는 기능이 있다. 이 기능을 활성화 시키기 위한 명령으로 올바른 것은?

① echo "1" > /proc/sys/net/ipv4/icmp_echo_broadcast_ignore

② echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

❸ echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

④ echo "1" > /proc/sys/net/ipv4/icmp_ignore_broadcasts

18. 래드햇 리눅스 6.0이 설치된 시스템에서 RPM 파일로 리눅스 6.0 CD-ROM 안에 들어있는 Apache 프로그램을 이용 웹 사이트를 운영하고 있다. linuxuser 라는 일반 사용자가 자기 홈 디렉토리 하위에 public_html 이라는 디렉토리를 만들고 자기 개인 홈페이지를 만들었는데, 이 홈페이지에 접속하려면 웹 브라우저에서 URL을 어떻게 입력해야 하는가? (서버의 IP는 192.168.1.1 이다.)

① http://192.168.1.1/

② http://192.168.1.1/linuxuser/

③ http://192.168.1.1/-linuxuser/

❹ http://192.168.1.1/~linuxuser/

19. 기존 유닉스 운영체제 같은 경우 사용자의 암호와 같은 중요한 정보가 /etc/passwd 파일안에 보관되기 때문에 이 파일을 이용해서 해킹을 하는 경우가 있었다. 이를 보완하기 위해서 암호정보만 따로 파일로 저장하는 방법이 생겼는데, 이 방식의 명칭은?

① DES Password System

② RSA Password System

③ MD5 Password System

❹ Shadow Password System

20. 한시간에 한번씩 특정한 명령을 수행하고자 할 때 래드햇 리눅스는 어떤 디렉토리 하위에 실행할 명령이 담긴 스크립트를 위치시켜야하는가?

① /etc/cron.hourly

❷ /var/cron/cron.hourly

③ /etc/cron/cron.hourly

④ /etc/rc3.d

21. WU-FTP 서버에서 특정 사용자의 FTP 로그인을 중지시키기 위해서 설정해야할 파일은?

① ftpcount

② ftpwho

③ hosts.deny

❹ ftpusers

22. netstat -an 명령으로 시스템의 열린 포트를 확인한 결과 31337 포트가 리눅스 상에 열려 있음을 확인하였다. 어떤 프로세스가 이 31337 포트를 열고 있는지 확인하려면 어떤 명령을 이용해야 하는가?

❶ fuser

② nmblookup

③ inetd

④ ps

23. 어떤 시스템의 messages 로그파일의 일부이다. 로그파일의 분석이 잘못된 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.

❸ 8월 28일 gozila라는 id로 누군가 접속하여 firewall.txt 파일을 다운 받아갔다.

④ batman 이라는 사람이 8월 28일에 su 명령을 사용하여 root 권한을 얻었다.

24. 다음은 어떤 시스템의 ifconfig 내용을 본 결과이다. 해설이 틀린 것은?

```
eth0 Link encap:Ethernet HWaddr
00:A0:24:A0:AC:10
 inet addr:192.168.1.254 Bcast:192.168.1.255
Mask:255.255.
   255.0
 UP BROADCAST RUNNING MULTICAST
MTU:1500 Metric:1
 RX packets:82860 errors:3 dropped:0 overruns:0
frame:3
 TX packets:84896 errors:0 dropped:0 overruns:0
carrier:5334
 collisions:3746 txqueuelen:100
 Interrupt:9 Base address:0x300
 lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 UP LOOPBACK RUNNING MTU:3924 Metric:1
 RX packets:172 errors:0 dropped:0 overruns:0
frame:0
 TX packets:172 errors:0 dropped:0 overruns:0
carrier:0
 collisions:0 txqueuelen:0
 ppp0 Link encap:Point-to-Point Protocol
 inet addr:210.111.175.88 P-t-P:211.39.49.25
Mask:255.255.
  255.255
 UP POINTOPOINT RUNNING NOARP MULTICAST
  MTU:1514 Metric:1
 RX packets:1467 errors:0 dropped:0 overruns:0
frame:0
 TX packets:1328 errors:0 dropped:0 overruns:0
carrier:0
 collisions:0 txqueuelen:10
```

① ppp로 받은 내 IP 주소는 210.111.175.88 이다.

❷ ppp로 받은 내 IP 주소는 211.39.49.25 이다.

③ 리눅스의 Ethernet 주소는 192.168.1.254 이다.

④ lo는 loopback device를 의미한다.

25. 다음 IP 프로토콜의 어드레스에 관한 설명 중 틀린 것은?

❶ IP어드레스는 32bit 구조를 가지고 A, B, C, D의 4종류의 클래스로 구분한다.

② 127.0.0.1은 루프백 테스트를 위한 IP주소라고 할 수 있다.

③ 클래스 B는 중간 규모의 네트워크를 위한 주소 클래스로 네트워크 ID는 129~191 사이의 숫자로 시작한다.

④ 클래스 C는 소규모의 네트워크를 위한 주소 클래스로 네트워크 당 254개의 호스트만을 허용한다.

26. 래드햇 리눅스에 기본으로 제공되는 Bind 8.2 버전의 DNS 시스템에서 Zone 파일에 아래와 같은 구문이 있다. 여기서 두번째 라인(IN MX 20 smtp.hitel.net.)의 역할은?

```
IN MX 10 pop3
IN MX 20 smtp.hitel.net.
```

① 메일을 받을때 pop3 메일서버가 응답이 없으면 smtp.hitel.net 메일서버가 대신 받는다.

② 메일을 받을때 pop3 메일서버 먼저 메일이 배달되고 나중에 smtp.hitel.net 메일서버가 또 받는다.

❸ 메일을 받을때 pop3 메일서버가 응답이 없으면 smtp.hitel.net 메일서버에 임시 저장된다.

④ 메일을 보낼때 pop3 메일서버와 smtp.hitel.net 메일서버 중 부하가 적은 쪽으로 메일을 보낸다.

27. 당신은 linuxman의 계정을 비밀번호가 없이 로그인 되도록 만들려고 한다. 당신의 linux서버는 shadow password system을 사용하고 있고, /etc/passwd에서 linuxman의 부분은 다음과 같다. 어떻게 해야 비밀번호없이 로그인 할 수 있는가?

```
linuxman:x:500:500::/home/bonnung:/bin/bash
```

① /etc/passwd파일의 linuxman의 두번째 필드를 공백으로 만든다.

❷ /etc/shadow파일의 linuxman의 두번째 필드를 공백으로 만든다.

③ /etc/passwd파일의 linuxman의 다섯번째 필드를 "!!"으로 채운다.

④ root로 로그인하여 passwd linuxman 명령으로 비밀번호를 바꾼다.

28. Windows 2000 Sever에서 지원하는 PPTP (Point to Point Tunneling Protocol)에 대한 설명으로 잘못된 것은?

❶ PPTP 헤드 압축을 지원한다.

② IPsec를 사용하지 않으면 터널인증을 지원하지 않는다.

③ PPP 암호화를 지원한다.

④ IP 기반 네트워크에서만 사용가능하다.

29. 다음 중 Windows 2000 서버에서 감사정책을 설정하고 기록을 남길수 있는 그룹은?

❶ Administrators

② Security operators

③ backup operators

④ audit operators

30. Windows 98 Client에서 컴퓨터이름이 testsrv 라고 설정되어 있는 Windows 2000 서버의 c:\winnt 폴더에 접근하고자 한다. testsrv 서버는 관리자가 C:\winnt 디렉토리 공유를 설정하여 놓지 않은 상태이다. 관리목적용 기본 공유설정을 이용해서 testsrv 서버의 C:\winnt 폴더에 접근할 수 있는 올바른 방법은?

① 관리목적용 공유를 이용하더라도 서버에 디렉토리는 접근할 수 없다.

❷ Windows 98 실행창에서 \\testsrv\admin$을 입력하여 접근한다.

③ Windows 98 실행창에서 \\testsrv\winnt를 입력하여 접근한다.

④ Windows 98 실행창에서 \\testsrv\netlogon을 입력하여 접근한다.

【3과목】 네트워크 (15문제)

31. 다음 중 Windows 2000 서버 운영체제에서 이벤트를 감사할 때 감사할 수 있는 항목이 아닌 것은?

① 파일 폴더에 대한 액세스

② 사용자의 로그온과 로그오프

❸ 메모리에 상주된 프로세스의 사용빈도

④ 액티브 디렉토리에 대한 변경시도

32. Media Access Control 프로토콜과 Logical Link Control 프로토콜은 OSI 7계층 중 몇 번째 계층에 속하는가?

① 1 계층

❷ 2 계층

③ 3 계층

④ 4 계층

33. 네트워크 장비 중 Layer 2 스위치가 의미하는 것은?

① 포트기반의 스위칭

❷ Media Access Control Address 기반의 스위칭

③ IP 주소기반의 스위칭

④ 컴퓨터이름을 기반으로 한 스위칭

34. 방화벽에서 내부 사용자들이 외부 FTP에 자료를 전송하는 것을 막고자 한다, 외부 FTP에 Login은 허용하되, 자료전송만 막으려면 다음 중 몇 번 포트를 필터링 해야 하는가?

① 23

② 21

❸ 20

④ 25

35. TCP는 연결 설정과정에서 3-way handshaking 기법을 이용하여 호스트 대 호스트의 연결을 초기화 한다. 다음 중 호스트 대 호스트 연결을 초기화할 때 사용되는 패킷은?

❶ SYN

② RST

③ FIN

④ URG

36. 다음 중 TCP/IP Sequence Number(순서번호)가 시간에 비례하여 증가하는 운영체제는?

① HP-UX

② Linux 2.2

❸ MS Windows

④ AIX

37. TCP/IP 프로토콜을 이용해 클라이언트가 서버의 특정포트에 접속을 하려고 할 때 서버가 해당포트를 열고 있지 않다면 응답 패킷의 코드비트에 특정 비트를 설정한 후 보내 접근할 수 없음을 통지하게 된다. 다음 중 클라이언트가 서버의 열려있지 않은 포트에 대한 접속에 대해 서버가 보내는 응답패킷의 코드비트 내용이 올바른 것은?

① SYN

② ACK

③ FIN

❹ RST

38. IPv4 패킷의 헤더에 DF비트가 1 로 설정이 되어있는 10000 바이트의 UDP 패킷을 MTU가 1500으로 설정되어 있는 네트워크에 속한 라우터에게 전달하였을 때 일반적으로 예상되는 라우터의 반응은?

① 알맞는 MTU 크기로 패킷을 자른 후 전송한다.

② 패킷을 재조합한다.

❸ 패킷을 자를 수 없다는 오류를 발생시킨다.

④ 라우터의 모든 동작이 중단되며, 재부팅이 필요해진다.

39. TCP/IP 프로토콜을 이용해서 서버와 클라이언트가 통신을 할 때, Netstat 명령을 이용해 현재의 접속상태를 확인할 수 있다. 클라이언트와 서버가 현재 올바르게 연결되어 통신중인 경우 netstat으로 상태를 확인하였을 때 어떤 메시지를 확인할 수 있는가?

① SYN_PCVD

❷ ESTABLISHED

③ CLOSE_WAIT

④ CONNECTED

40. TCP의 header의 구성은?

❶ 각 32비트로 구성된 6개의 단어

② 각 6비트로 구성된 32개의 단어

③ 각 16 비트로 구성된 7개의 단어

④ 각 7비트로 구성된 16개의 단어

41. 다음 중 IGRP(Interior Gateway Routing Protocol)의 특징이 아닌 것은?

① 거리벡터 라우팅 프로토콜.

② 메트릭을 결정할 때 고려요소 중 하나는 링크의 대역폭이 있다.

③ 네트워크 사이의 라우팅을 최적화에 효율적.

❹ 링크상태 프로토콜로 메트릭의 비용을 이용한 라우팅.

42. Broadcast and Multicast의 종류와 그에 대한 설명으로 옳지 않은 것은?

① unicast - 메시지가 임의의 호스트에서 다른 호스트로 전송되는 방식을 말한다.

② broadcast - 메시지가 임의의 호스트에서 네트워크상의 모든 호스트에 전송되는 방식을 말한다.

③ multicast - 메시지가 임의의 호스트에서 네트워크 상의 특정 호스트(Group)에 전송되는 방식을 말한다.

❹ broadcast - 메시지가 네트워크 상의 모든 호스트로부터 임의의 호스트에 전송되는 방식을 말한다.

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

43. 다음 중 T3회선에서의 데이터 전송속도는?

❶ 45Mbps

② 128Kbps

③ 1.544Mbps

④ 65.8Mbps

44. 방화벽의 세 가지 기능이 아닌 것은?

① 패킷필터링(packet filtering)

② NAT(Network Address Translation)

❸ VPN(Virtual Private Network)

④ 로깅(logging)

45. 다음 중 알려진 취약점을 알아보는 스캐너의 종류가 아닌 것은?

① SAINT

② MSCAN

③ ISS

❹ Squid

【4과목】 보안 (15문제)

46. DoS (Denial of Service) 의 개념과 거리가 먼 것은?

① 다량의 패킷을 목적지 서버로 전송하여 서비스를 불가능하게 하는 행위

② 로컬 호스트의 프로세스를 과도하게 fork 함으로서 서비스에 장애를 주는 행위

③ 서비스 대기중인 포트에 특정 메세지를 다량으로 보내 서비스를 불가능하게 하는 행위

❹ 익스플로잇을 사용하여 특정권한을 취득하는 행위

47. IIS를 통하여 Web서비스를 하던 중 .asp 코드가 외부 사용자에 의하여 소스코드가 유출되는 버그가 발생하였다. 기본적으로 취해야 할 사항이 아닌 것은?

① 중요 파일(global.asa 등)의 퍼미션을 변경 혹은 파일수정을 통하여 외부로부터의 정보유출 가능성을 제거한다.

② .asp의 권한을 실행권한만 부여한다.

❸ C:\WINNT\System32\inetsrv\asp.dll에 매칭되어있는 .asp를 제거한다.

④ .asp가 위치한 디렉토리와 파일에서 Read 권한을 제거한다.

48. 다음 중 32비트 IP주소를 48비트 이더넷 주소로 변환하는 프로토콜은?

❶ ARP

② RARP

③ IGMP

④ ICMP

49. 버퍼 오버 플로우(Buffer Overflow) 개념으로 틀린 것은?

① 스택의 일정부분에 익스플로잇 코드(exploit code)를 삽입하고 어떤 프로그램의 리턴 어드레스(return address)를 익스플로잇 코드(exploit code)가 위치한 곳으로 돌린다.

② 대체적으로 문자열에 대한 검사를 하지 않아서 일어나는 경우가 많다.

③ 소유자가 root인 setuid가 걸린 응용프로그램인 경우 익스플로잇 코드(exploit code)를 이용 root의 권한을 획득할 수 있다.

❹ main 프로그램과 sub 프로그램의 경쟁관계와 setuid를 이용하여 공격하는 패턴이 존재한다.

50. IIS 서비스에서 현재까지 나타난 취약점이 아닌 것은?

① %aa %ee (지정된 URL 뒤에 %aa 등을 기입함으로서 소스코드 유출)

② Unicode Bug (유니코드를 이용하여 웹 서비스 상위의 디렉토리나 파일에 접근가능)

❸ wtr Bug(global.asa같은 특정파일의 URL에 +.wtr를 적어줌으로서 권한이 없는 디렉토리나 파일상에 접근가능)

④ ::$DATA(asp 같은 보이지 않는 코드에 ::$data를 적어줘서 소스코드 유출)

51. 다음 중 SSL (Secure Socket Layer)의 개념이 아닌 것은?

① 연결시에 클라이언트와 서버는 전송중인 데이터를 암호화하기 위해 비밀키를 교환한다. 그러므로 도청되더라도 암호화 되어있어 쉽게 밝혀낼 수 없음.

❷ 클라이언트는 서버에게 접속시 인증서를 요구하고 자신의 비밀키를 이용한 암호화 방식으로 데이터를 암호화하여 전송하므로 스니핑의 방지가 가능.

③ 공용키 암호화를 지원하기 때문에 RSA나 전자서명표준 같은 방법을 이용하여 사용자를 인증할 수 있음.

④ MD5나 SHA같은 메시지 다이제스트 알고리즘을 통해서 현재 세션에 대한 무결성검사를 할 수 있기 때문에 세션을 가로채는 것을 방지할 수 있음.

52. 다음은 인바운드 서비스 이용에 대한 주요한 위험 요소의 설명이다. 거리가 먼 것은?

① 하이재킹 - 시스템에 사용자가 인증을 받은 후 누군가가 그 연결(session)을 훔치는 것

❷ 파일 크랙 - 암호가 걸린 대외비의 정보 파일을 누군가가 암호를 깨뜨리고 정보를 읽어내는 것

③ 패킷 스니핑 - 대외비의 데이터가 네트워크를 통과할 때 데이터의 간섭 없이 누군가가 그 데이터를 읽는 것

④ 잘못된 인증 - 시스템이 정당하지 않은 사용자를 정당한 사용자로 확신하는 것

53. 커널버전 2.2. 에서 다음 스크립트의 역할은?

```
for $rp in /proc/sys/net/ipv4/conf/*/rp_filter
do
echo "1" > $rp
done
```

① 각 랜카드의 포트 필터링 기능을 활성화 한다.

② 각 랜카드의 IP 필터링 기능을 활성화 한다.

③ 각 랜카드의 ARP Spoofing 방지 기능을 활성화 한다.

❹ 각 랜카드의 IP Spoofing 방지 기능을 활성화 한다.

54. Ipchains 프로그램을 이용해서 192.168.1.1 의 80 번 포트로 향하는 패킷이 아닌 것을 모두 거부하고 싶을 때 input 체인에 어떤 명령을 이용해서 설정해야 하는가?

❶ ipchains -A input -j DENY -d ! 192.168.1.1 80

② ipchains -A input -j DENY -d 192.168.1.1 ! 80

③ ipchains -A input -j DENY -s ! 192.168.1.1 80

④ ipchains -A input -j DENY -s 192.168.1.1 ! 80

55. Nmap의 옵션 중 상대방의 OS를 알아내는 옵션은?

❶ [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 -Os www.target.com

56. 시스템 상에서 Rootkit의 역할이 아닌 것은?

① 불법적인 권한을 다시 획득하는 역할을 수행한다.

② 시스템상에서 침입자의 흔적을 지워주는 역할을 수행한다.

③ 정상적인 프로그램처럼 보이지만 내부에 악의적인 코드가 내장되어있다.

❹ 자가복제를 통해 자신의 존재를 숨기면서 다른 시스템과 다른 접속을 시도한다.

57. TCPdump라는 프로그램을 이용해서 192.168.1.1 호스트로부터 192.168.1.10 이라는 호스트로 가는 패킷을 보고자 한다. 올바른 명령은?

① tcpdump src host 192.168.1.10 dst host 192.168.1.1

② tcpdump src host 192.168.1.1 dst host 192.168.1.10

❸ tcpdump src host 192.168.1.1 and dst host 192.168.1.10

④ tcpdump src host 192.168.1.10 and dst host 192.168.1.1

58. 다음 내용 중 내부점검 도구명과 그 기능이 맞는 것으로 묶여진 것은?

ㄱ. Trpwire -시스템상의 파일 무결성 검사 ㄴ. COPS - 중요 파일들에 대한 CRC 검사 ㄷ. Tiger - 유닉스 시스템내의 보안문제 검색하는 스크립트 ㄹ. Crack - 취약한 패스워드 크랙툴

① ㄱ

② ㄱ,ㄷ

③ ㄱ,ㄷ,ㄹ

❹ ㄱ,ㄴ,ㄷ,ㄹ

59. 다음 내용은 보안 운영체제의 특정한 보안기능에 대해 설명한 것이다. 어떤 기능을 말하고 있는가?

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 보호되어야 한다.

① 사용자 식별 또는 인증

❷ 감사 및 감사 기록

③ 강제적/임의적 접근 통제

④ 침입탐지

60. DDoS(Distrivuted Denial of Service)로 알려진 프로그램이 아닌 것은?

① Trinoo

② TFN

③ Stacheldraft

❹ Teardrop