2025년04월20일년 인터넷보안전문가 2급 필기시험 기출문제 답안

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

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

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

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

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. IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?

① 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.

② 기밀성 기능은 AH(Authentication Header)에 의하여 제공되고, 인증 서비스는 ESP(Encapsulating Security Payload)에 의하여 제공된다.

③ 보안 연계(Security Association)는 사용된 인증 및 암호 알고리즘, 사용된 암호키, 알고리즘의 동작 모드 그리고 키의 생명 주기 등을 포함한다.

④ 키 관리는 수동으로 키를 입력하는 수동방법과 IKE 프로토콜을 이용한 자동방법이 존재한다.

2. 다음 중 네트워크 및 인터넷 보안 프로토콜(예: TLS, IPsec 등)을 정의하고 표준화하는 대표적인 국제 표준화 기구는?

① IEEE (Institute of Electrical and Electronics Engineers)

② ITU (International Telecommunication Union)

③ IETF (Internet Engineering Task Force)

④ ISO (International Organization for Standardization)

3. 다음 중 포트 기반 취약점을 악용해 빠르게 확산되며, 메모리에 상주하고 네트워크 트래픽 과부하를 유발하여 DNS 장애 및 인터넷 접속 지연을 초래한 웜 공격 사례는?

① Michelangelo

② Trojan Horse

③ SQL Slammer

④ WannaCry

4. 다음 중 비대칭형 암호화 방식(Asymmetric Encryption) 또는 공개키 기반 키 교환을 위한 알고리즘으로 가장 적절한 것은?

① AES (Advanced Encryption Standard)

② SEED (Secure Encryption and Decryption)

③ ECDSA (Elliptic Curve Digital Signature Algorithm)

④ ECDH (Elliptic Curve Diffie-Hellman)

5. 다음과 같은 공격 기법으로 가장 적절한 것은?

> 한 금융기관의 직원이 고객센터에서 발송된 것처럼 보이는 이메일을 수신했으나, 확인 결과 이는 공격자가 발신자 정보를 조작한 위장 이메일이었다. 이메일 내 링크 클릭 시 악성코드가 설치되어 정보 유출이 발생했으며, 해당 메일의 발신자는 실제 존재하지 않는 주소로 확인되었다.

① Packet Sniffing

② Email Spoofing

③ Man-in-the-Middle

④ SQL Injection

6. 다음과 같은 상황일 때, 보안 서비스 관점에서 가장 핵심적으로 요구되는 기능은?

> A 기업의 인사팀 직원은 내부 포털을 통해 전자서명을 포함한 계약서를 외부 협력사에 이메일로 전송했다. 그러나 이후 협력사는 해당 계약서의 수신 내역이 기록되지 않았으며, 전송된 문서의 정당성에 대해 의문을 제기했다.

① 비밀성 (Confidentiality)

② 무결성 (Integrity)

③ 부인방지 (Non-repudiation)

④ 접근제어 (Access Control)

7. 다음 지문과 관련하여 보안 정책에 가장 적합한 시스템 관리자의 조치는?

> A 시스템 관리자는 신규 리눅스 서버를 구축한 뒤, 사용자 요청이 다양할 것을 우려해 다수의 데몬과 서비스를 기본값 그대로 실행 상태로 두었다. 며칠 뒤, 보안 담당자는 IDS에서 다수의 포트 스캔 탐지 및 알려지지 않은 서비스에 대한 외부 접근 시도를 보고했다.

① 보안 설정과 관계없이 서비스 접근성 향상을 위해 모든 데몬을 계속 유지한다.

② 침입 탐지 로그는 참고용으로만 보고, 운영 중인 서비스는 유지한다.

③ 현재 실행 중인 서비스 목록을 점검하고, 불필요한 데몬은 중지하거나 제거한다.

④ 해당 서버의 방화벽 설정을 해제하고, 외부 접근 제한을 해제하여 테스트를 우선 수행한다.

8. 금융기관 또는 인터넷 환경에서 다수 사용자로부터 소액을 반복적으로 탈취하며, 피해자가 사건을 쉽게 인지하지 못하는 컴퓨터 사기 수법은?

① Scavenging

② 논리 폭탄(Logic Bomb)

③ 살라미(Salami) 기법

④ 자료의 부정변개(Data Diddling)

9. 다음 중 비대칭키 암호 시스템의 사용자 수(n)에 따른 키 관리 특징으로 가장 적절한 설명은?

① 비대칭키 시스템에서는 각 사용자 간 통신을 위해 사용자 수만큼의 공통 비밀키가 필요하다.

② 비대칭키 암호 시스템은 사용자 수와 관계없이 하나의 키만으로 모든 사용자가 통신할 수 있다.

③ 모든 사용자는 서로의 개인키를 공유해야 안전한 통신이 가능하다.

④ 사용자 1명당 1쌍의 키(공개키/개인키)가 필요하며, 전체 키 개수는 2n개이다.

10. 온라인 전자상거래에서 신용카드 결제 시, 사용자의 본인 인증을 강화하여 무단 결제 및 사기 거래를 방지하기 위해 널리 사용되는 보안 기술은?

① TLS

② 3D Secure

③ S/MIME

④ PGP

【2과목】운영체제 (20문제)

11. Linux 시스템에서 '/dev' 디렉터리에 대한 설명으로 가장 적절하지 않은 것은?

① 이 디렉터리는 실제 하드디스크에 저장된 정적 파일이 아니라, 운영체제가 부팅되거나 장치가 연결될 때 동적으로 생성되는 장치 파일이 위치하는 가상 디렉터리이다.

② 디바이스 파일은 장치 드라이버에 의해 생성되며, udev와 같은 디바이스 매니저가 이를 동적으로 관리한다.

③ 하드웨어 장치와 연동되는 실행 가능한 드라이버 프로그램들이 직접 이 디렉터리에 저장된다.

④ '/dev/null, /dev/zero, /dev/random' 등은 물리적 장치가 아닌, 커널에서 특별한 용도로 제공하는 가상 장치 파일이다.

12. 전통적인 Linux 시스템에서, 시스템 부팅 시 가장 먼저 실행되어 PID 1번을 차지하고, '/etc/inittab' 파일을 읽어 실행 레벨(runlevel)을 결정한 뒤, 서비스들을 시작하는 등 시스템 초기화를 직접 수행하는 프로세스는?

① telinit

② init

③ systemctl

④ rc.d

13. 다음 중 Linux의 커널이 직접적으로 수행하지 않는 기능은?

① 메모리 보호 및 할당

② 파일 시스템 접근 제어

③ 명령어 해석 및 실행

④ 프로세스 상태 전환 및 스케줄링

14. Linux 시스템에서 마운트된 각 파일시스템의 전체 용량, 사용 중인 용량, 남은 용량을 확인할 수 있는 명령어는?

① du

② df

③ lsblk

④ mount

15. 관리자가 새로운 SSD 디스크 '/dev/sdb'를 서버에 추가한 후, 파티션을 생성하기 위해 실행해야 할 명령어로 가장 적절한 것은?

① mount /dev/sdb1 /mnt

② mkfs.ext4 /dev/sdb1

③ fdisk /dev/sdb

④ lsblk /dev/sdb

16. 시스템 성능 저하가 발생한 Linux 서버에서 관리자가'free -h' 명령어를 실행하였다. 이 명령어를 사용하는 주요 목적으로 가장 적절한 것은?

① 디스크의 파티션 구조를 확인하기 위해

② 파일 시스템의 사용량을 점검하기 위해

③ 프로세스 목록을 확인하기 위해

④ 메모리 및 스왑의 사용 현황을 점검하기 위해

17. Linux 기반의 BIND DNS 서버에서 'example.com' 도메인의 zone 파일을 설정 중인 한 관리자는, SOA 레코드를 작성하면서 DNS 동작 오류를 방지하기 위한 설정 원칙을 검토하고 있다. 다음 중 SOA 레코드 설정 시 반드시 지켜야 할 사항으로 가장 적절한 것은?

① SOA 레코드는 zone 파일 맨 아래에 작성해야 하며, 다른 레코드보다 나중에 정의해야 한다.

② 하나의 도메인(zone)에는 슬레이브 DNS 서버 수만큼 SOA 레코드를 각각 따로 설정해야 한다.

③ SOA 레코드의 Serial 번호는 변경할 필요 없이 고정된 값을 사용해도 된다.

④ SOA 레코드는 zone 파일 맨 처음에 1개만 작성되어야 하며, Serial 값은 변경 시마다 증가해야 한다.

18. 한 시스템 관리자가 Apache 웹 서버의 보안을 강화하기 위해 'httpd.conf' 파일을 검토하고 있다. 다음 중 보안상 가장 바람직하지 않은 설정은?

① 웹 서버가 실행되는 사용자 계정(User)을 제한된 권한의 전용 계정으로 설정한다.

② DocumentRoot 디렉터리에 불필요한 실행 권한을 제거하고 필요한 파일만 배치한다.

③ 웹 서버가 사용할 User와 Group 값을 모두 root로 설정하여 파일 접근 권한 문제를 방지한다.

④ 접근 제어를 위해 특정 디렉터리에 '.htaccess' 파일을 활용하고 AllowOverride 지시어를 적절히 사용한다.

19. Linux에서 IP 주소를 호스트 이름으로 직접 연결할 때 사용하는 파일은?

① /etc/resolv.conf

② /etc/hosts

③ /etc/hostname

④ /etc/network/interfaces

20. Linux 서버의 포트 상태 점검 결과, 다음과 같은 두 개의 포트가 열린 것이 확인되었다. 관리자는 보안 강화를 위해 이 중 하나의 서비스를 즉시 비활성화하려고 한다. 보안상 가장 우선적으로 종료해야 할 서비스의 설명으로 적절한 것은?

```
tcp   0   0   0.0.0.0:23    0.0.0.0:*   LISTEN
tcp   0   0   0.0.0.0:22    0.0.0.0:*   LISTEN
```

① 22번 포트의 서비스는 명령어 기반 원격 접속을 지원하지만, 기본적으로 암호화되지 않아 정보 유출 위험이 있다.

② 23번 포트의 서비스는 사용자 인증 정보가 암호화 없이 전송되므로 계정 탈취 위험이 높아 즉시 차단하는 것이 바람직하다.

③ 22번 포트의 서비스는 외부에서 접근할 수 있으므로 반드시 서비스 자체를 제거해야 한다.

④ 23번 포트는 오래된 시스템 관리용 포트이므로 그대로 유지하는 것이 일반적이다.

21. Linux에서 root 유저로 로그인 한 후 'cp -rf /etc/* ~/temp' 라는 명령으로 복사를 하였는데, 여기서 '~' 문자가 의미하는 뜻은?

① /home 디렉터리

② /root 디렉터리

③ root 유저의 home 디렉터리

④ 현재 디렉터리의 하위라는 의미

22. 시스템 관리자가 다음과 같은 명령어를 실행했다. 이 명령어에 대한 설명으로 가장 적절한 것은?

```
nice -n 10 myscript.sh
```

① myscript.sh를 PID 10번으로 실행하며, 자동으로 10초 후 종료된다.

② myscript.sh를 기존보다 높은 우선순위로 실시간 스케줄링 정책에 따라 실행한다.

③ myscript.sh를 기본 우선순위보다 낮게 설정하여 실행한다.

④ myscript.sh를 실행 중인 프로세스로 간주하고 현재 우선순위를 변경한다.

23. Linux 명령어 'mv [옵션] file1 file2'에서, file2가 이미 존재하는 경우 덮어쓸 것인지 여부를 사용자에게 묻는 옵션은?

① -f

② -i

③ -v

④ -n

24. Linux 서버에서 파일의 권한 모드가 '-rwxr---w-'로 설정되어 있다. 이 설정을 실무적으로 검토할 때, 가장 중요한 보안 점검 항목은?

① 소유자가 모든 권한을 가지고 있으므로, 관리자만 접근 가능하다.

② 동일 그룹에 실행 권한을 부여하지 않고, 읽기 권한만 부여하여 불필요한 실행을 방지한다.

③ 다른 사용자에게 쓰기 권한만 부여하여 실행 권한을 부여하지 않으므로 안전하다.

④ 파일이 너무 많은 사용 권한을 가지지 않도록, 'chmod 700'으로 변경하여 불필요한 권한을 차단한다.

25. Windows Server에서 Administrator 계정의 보안을 강화하려고 한다. 다음 중 Administrator 계정에 대해 권장되는 보안 설정으로 옳지 않은 것은?

① Administrator 계정의 이름을 변경하여 알 수 없도록 한다.

② Administrator 계정에 대해 강력한 비밀번호 정책을 적용한다.

③ Administrator 계정에 대해 로컬 그룹 정책에서 최소 로그인 시도 횟수를 설정한다.

④ Administrator 계정에 대해 원격 로그인을 비활성화하여 보안성을 강화한다.

26. Linux에서 'ls -al' 명령에 의하여 출력되는 정보로 옳지 않은 것은?

① 파일의 접근허가 모드

② 파일 이름

③ 소유자명, 그룹명

④ 파일의 소유권이 변경된 시간

27. 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.

28. 다음 중 파일 시스템에 대한 설명으로 옳지 않은 것은?

① ZFS는 데이터 중복 제거와 압축 기능을 제공하며, 데이터 무결성과 파일 시스템 스냅샷을 지원한다.

② Btrfs는 파일 시스템 복구 기능을 지원하며, 디스크 오류 복구와 유연한 스냅샷 기능을 제공한다.

③ F2FS는 플래시 기반 저장 장치(예: SSD)에 최적화되어 있으며, 속도 향상을 목표로 개발된 파일 시스템이다.

④ EXT4는 기존의 안정적인 파일 시스템으로, ZFS와 같은 고급 기능을 제공하여 데이터 복구, 데이터 중복 제거 등의 기능을 제공한다.

29. IIS 웹 서버를 설치한 다음에는 기본 웹사이트 등록정보를 수정하여야 한다. 웹사이트에 접속하는 동시 접속자수를 제한하려고 할 때 어느 부분을 수정해야 하는가?

① 성능 탭

② 연결 수 제한

③ 연결 시간 제한

④ 문서 탭

30. Linux에서 특정한 파일을 찾고자 할 때 사용하는 명령어는?

① mv

② cp

③ find

④ file

【3과목】 네트워크 (15문제)

31. IP 주소와 서브넷 마스크의 역할에 대한 설명으로 옳지 않은 것은?

① IP 주소는 호스트가 속한 네트워크를 구분하고, 각 장치에 고유한 식별자로 사용된다.

② 서브넷 마스크는 네트워크 주소와 호스트 주소를 구분하는 데 사용된다.

③ IP 주소와 서브넷 마스크를 함께 사용하여 호스트가 속한 네트워크 범위를 결정할 수 있다.

④ 서브넷 마스크는 IP 주소를 클래스 A, B, C로 나누는데 사용된다.

32. 다음 중 TCP와 UDP의 차이점에 대한 설명으로 옳지 않은 것은?

① TCP는 연결형 프로토콜로, 데이터 전송 전에 연결을 설정하고, 신뢰성 있는 전송을 보장한다.

② UDP는 비연결형 프로토콜로, 연결 설정 없이 데이터를 전송하며, 신뢰성 없는 전송을 한다.

③ TCP는 패킷 순서 보장과 흐름 제어, 오류 검출을 제공하지만, 속도가 느리다.

④ UDP는 데이터 흐름 제어와 오류 검출을 제공하여, 신뢰성 있는 전송을 보장한다.

33. TCP/IP 모델에서 각 계층의 주요 역할에 대한 설명으로 옳지 않은 것은?

① 응용 계층은 데이터 송수신을 담당하며, HTTP, FTP, DNS와 같은 프로토콜이 이 계층에 포함된다.

② 인터넷 계층은 IP 주소 지정 및 라우팅을 담당하며, IP 프로토콜이 대표적이다.

③ 전송 계층은 데이터 전송의 신뢰성을 보장하고, TCP와 UDP가 포함된다.

④ 네트워크 액세스 계층은 네트워크 연결에 필요한 세션 관리를 담당한다.

34. 다음 조건에 가장 적합한 네트워크 토폴로지 구성 방식은?

> 한 중견기업의 IT 관리자는 본사의 네트워크를 다음과 같은 조건으로 재설계하려고 한다.
> - 각 부서(인사, 회계, 연구소)는 서로 독립된 연결망을 갖되, 중앙 서버실을 통해 상호 통신이 가능해야 한다.
> - 부서 간 데이터 전송은 중앙에서 제어하고, 부서 내 문제가 전체에 영향을 주지 않도록 해야 한다.
> - 추후 부서가 추가되거나 사용자가 늘어나더라도 손쉽게 확장 가능해야 한다.

① 버스(Bus)

② 링(Ring)

③ 스타(Star)

④ 메쉬(Mesh)

35. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?

① SNMP v1은 RFC(Request For Comment) 1157에 정의되어 있다.

② 네트워크 장비의 성능, 상태, 구성 값을 조회하거나 설정하는 데 사용된다.

③ 기본적으로 TCP 연결 기반의 세션을 통해 데이터를 송수신한다.

④ SNMP v3에서는 인증과 암호화를 통한 보안 기능이 포함되어 있다.

36. IPv6 프로토콜의 주소 길이는 몇 비트인가?

① 32bit

② 64bit

③ 128bit

④ 256bit

37. TCP 헤더 필드의 내용으로 옳지 않은 것은?

① TTL(Time To Live)

② 발신지 포트번호

③ 윈도우 크기

④ Checksum

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. 데이터 링크 오류제어를 위한 ARQ 방식 중 오류가 발생한 프레임만을 재전송하는 방식으로, 전송 성능이 가장 우수한 것은?

① Stop-and-Wait ARQ

② Go-back-N ARQ

③ Selective Repeat ARQ

④ 모든 ARQ는 전송 성능이 동일하다.

40. TCP/IP 프로토콜을 이용해 클라이언트가 서버의 특정 포트에 접속하려고 할 때 서버가 해당 포트를 열고 있지 않다면 응답 패킷의 코드 비트에 특정 비트를 설정한 후 보내 접근할 수 없음을 통지하게 된다. 다음 중 이러한 비정상 연결 상황 처리에 사용되는 제어 비트는?

① SYN

② ACK

③ FIN

④ RST

41. 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.

42. 패킷(Packet)에 있는 정보로 옳지 않은 것은?

① 출발지 IP Address

② TCP 프로토콜 종류

③ 전송 데이터

④ 목적지 IP Address

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]

GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

43. TCP/IP 프로토콜을 이용한 네트워크상에서 병목현상(Bottleneck)이 발생하는 이유로 가장 옳지 않은 것은?

① 다수의 클라이언트가 동시에 호스트로 접속하여 다량의 데이터를 송/수신할 때

② 불법 접근자가 악의의 목적으로 대량의 불량 패킷을 호스트로 계속 보낼 때

③ 네트워크에 연결된 호스트 중 다량의 질의를 할 때

④ 호스트와 연결된 클라이언트 전체를 포함하는 방화벽 시스템이 설치되어 있을 때

44. 스위치 기반으로 운영되는 일반적인 이더넷 LAN 환경에 대한 설명으로 옳지 않은 것은?

① 스위치 기반 LAN은 포트 간 충돌이 발생하지 않으며, Full Duplex 통신이 가능하다.

② 스위치는 각 포트에 연결된 장치의 MAC 주소를 학습하여, 프레임을 효율적으로 전달한다.

③ 스위치는 계층적 구조로 구성되며, VLAN 기능을 통해 브로드캐스트 도메인을 논리적으로 분리할 수 있다.

④ 스위치 환경에서는 충돌 감지를 위해 CSMA/CD 기능이 반드시 활성화되어야 한다.

45. 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

【4과목】보안 (15문제)

46. 버퍼 오버플로우(Buffer Overflow)의 설명으로 옳지 않은 것은?

① 지정된 버퍼의 크기보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 만드는 것을 의미한다.

② 대부분의 경우 버퍼가 오버플로우 되면 프로그램이 비정상적으로 종료되면서 루트 권한을 획득할 수 있다.

③ 버퍼가 오버플로우 되는 순간에 사용자가 원하는 임의의 명령어를 수행시킬 수 있다.

④ 버퍼 오버플로우를 방지하기 위해서는 시스템에 최신 패치를 유지해야 한다.

47. Linux 서버 보안 점검 중, 내부 서비스에서 사용하지 않는 포트가 외부에서 접근 가능한 상태(LISTEN)로 확인되었다. 보안 담당자는 해당 포트를 차단하기 위해 firewalld를 사용하여 TCP 31337 포트를 외부에서 접근하지 못하도록 설정하려고 한다. 다음 중 정상적인 firewalld 명령어로서, 해당 포트를 즉시 차단할 수 있는 것은?

① firewall-cmd --add-port=31337/tcp --permanent

② firewall-cmd --remove-port=31337/tcp

③ firewall-cmd --reload

④ firewall-cmd —block-port=31337/tcp

48. 보안 담당자가 Linux 서버 점검 중, 정상적인 서비스에서 사용하지 않는 포트가 비정상적으로 열려 있는 것을 발견하였다. 이 포트를 열고 있는 프로세스의 이름과 PID 정보를 가장 정확하게 확인할 때 입력해야 하는 명령어는?

① netstat -r

② systemctl status network.service

③ ss -plnt

④ firewall-cmd --list-all

49. TLS(Transport Layer Security) 프로토콜에 대한 설명으로 옳지 않은 것은?

① TLS 1.3부터는 RSA 키 교환 방식으로 주로 사용되며, Handshake 중 세션 키를 암호화하여 전달한다.

② TLS에는 Handshake 프로토콜에서 생성되는 세션과, 그 세션 내에서 다수의 연결이 구성될 수 있다.

③ TLS Handshake 프로토콜은 통신 시작 시 암호화 방식 협상, 인증, 세션 키 생성을 수행한다.

④ TLS의 Record 계층은 데이터 분할, 무결성 확인을 위한 MAC 생성 및 첨부, 암호화 등의 기능을 수행한다.

50. 보안 담당자는 사내 Linux 서버에서 비정상적인 대량의 외부 접속 요청을 탐지하였다. 로그를 분석한 결과, 외부 IP 주소들이 내부 사설망 대역(예: 192.168.x.x, 10.x.x.x 등)을 출발지 주소로 사용하고 있는 것으로 나타났다. 이는 IP Spoofing 공격의 전형적인 징후로 판단된다. 다음 중 이러한 IP Spoofing 공격을 네트워크 차원에서 사전에 차단하는 가장 적절한 방법은?

① 서버에 설치된 DNS 캐시를 초기화하여 위조 IP를 제거한다.

② 라우터나 방화벽에서 내부 IP 대역을 출발지로 사용하는 외부 패킷을 차단하는 규칙을 설정한다.

③ 서버에서 HTTP 요청 로그를 삭제하여 접속 기록을 지운다.

④ 방화벽에서 포트 포워딩을 설정하여 외부 포트 접근을 모두 허용한다.

51. SYN 플러딩 공격에 대한 설명으로 옳은 것은?

① TCP 프로토콜의 3-way handshaking 방식의 접속 문제점을 이용하는 것으로, IP 스푸핑 공격을 위한 사전 준비 단계에서 이용되는 공격이며, 서버가 클라이언트로부터 과도한 접속 요구를 받아 이를 처리하기 위한 구조인 백로그(backlog)가 한계에 이르러 다른 클라이언트로부터 오는 새로운 연결 요청을 받을 수 없게 하는 공격이다.

② 함수의 지역변수에 매개변수를 복사할 때 길이를 확인하지 않은 특성을 이용하는 공격 방법이다.

③ 네트워크에 연결된 호스트들의 이용 가능한 서비스와 포트를 조사하여 보안 취약점을 조사하기 위한 공격방법이다.

④ 패킷을 전송할 때 암호화하여 전송하는 보안 도구이다.

52. Linux 서버에서 시스템 점검을 위해 root 사용자만 로그인 가능하도록 설정하고, 다른 일반 사용자 계정의 로그인을 일시적으로 차단하려고 한다. 이때 사용하는 설정 파일은?

① /etc/nologin

② /etc/hosts.allow

③ /etc/hosts.deny

④ /sbin/nologin

53. Linux 시스템에서 사용되는 파일 무결성 검사 도구인 Tripwire에 대한 설명으로 옳지 않은 것은?

① Tripwire는 어셈블리어로 작성되어 거의 모든 운영 체제에서 컴파일이 가능하다.

② 시스템 설치 후 초기 상태의 파일 해시 정보를 데이터베이스에 저장할 수 있다.

③ Tripwire는 정책 파일을 통해 감시할 디렉터리와 파일의 조건을 정의할 수 있다.

④ Tripwire는 무단 변경을 탐지하고 보고할 수 있도록 전자서명 기반의 데이터베이스 무결성 검사를 수행한다.

54. 보안 담당자 A씨는 내부 개발 서버에서 다음과 같은 이상 징후를 발견하였다. A씨는 이와 같은 불법 로그인 시도 및 인증 실패 내역을 추적하기 위해 가장 우선적으로 확인해야 할 로그 파일을 살펴보고자 한다. 다음 중 이 상황에서 가장 먼저 확인해야 할 로그 파일로 적절한 것은?

- 새벽 시간대에 존재하지 않는 사용자 계정으로 로그인 시도가 수차례 발생하였다.
- 일부 로그인 시도는 실패했고, 몇몇은 외부 IP에서 시도된 것으로 보인다.
- 해당 서버는 외부로 SSH 포트를 열어두고 있으며, 관리자는 비밀번호 인증 방식을 사용 중이다.

① /var/log/boot.log

② /var/log/auth.log

③ /var/log/dmesg

④ /var/log/cron

55. 다음은 PGP(Pretty Good Privacy) 기반 암호화 기술에 대한 설명이다. 오늘날에는 GNU Privacy Guard(GPG)와 같은 OpenPGP 표준 구현을 통해 널리 사용되고 있다. 이 암호화 방식의 보안 특성 중 옳지 않은 것은?

① PGP는 메시지 암호화에 대칭키를 사용하고, 이 대칭키를 수신자의 공개키로 암호화한다.

② PGP는 공개키 기반 전자서명을 통해 메시지의 무결성과 발신자 인증을 지원한다.

③ PGP는 키 인증을 중앙 인증기관(CA)을 기반으로 하는 방식으로 수행한다.

④ PGP는 이메일, 파일, 스크립트 등에 대한 암호화 및 서명 기능을 제공한다.

56. 정보보안팀은 사내 네트워크에 Snort를 도입해 실시간 침입 탐지 시스템(IDS)으로 운영 중이다. Snort는 사전에 정의된 탐지 규칙(Rule Set)에 따라 트래픽을 모니터링하고, 일치하는 패턴이 감지되면 특정 동작을 수행한다. 다음 중 Snort가 트래픽을 탐지한 후 기본적으로 수행할 수 없는 동작은?

① 탐지된 패킷에 대해 경고를 생성하여 관리자에게 알린다.

② 로그 파일에 패킷 정보를 기록하여 추후 분석에 활용한다.

③ 특정 규칙에 따라 탐지된 트래픽을 무시하도록 설정할 수 있다.

④ 이상 징후가 감지된 패킷의 전송을 지연시켜 방화벽과 연동한다.

57. 시스템 관리자인 A씨는 리눅스 서버에서 한 시간마다 시스템 자원 상태를 점검하는 스크립트를 자동으로 실행하고자 한다. 복잡한 서비스 설정 없이, Linux 시스템에서 가장 간단하고 보편적인 방식으로 작업을 자동화하려고 한다. 다음 중 A씨가 스크립트를 배치할 위치로 가장 적절한 디렉터리는?

① /etc/cron.hourly

② /etc/init.d

③ /etc/fstab

④ /etc/profile

58. 보안 담당자는 사내 네트워크에서 이상하게 많은 ARP 패킷과 불규칙한 DNS 요청이 발생하는 것을 감지하고, 누군가 스니핑 또는 ARP Spoofing을 시도하고 있다고 의심하고 있다. 이에 따라 패킷 캡처 도구를 이용해 실시간 트래픽을 분석하고자 할 때 가장 적합한 도구는?

① Nikto

② John the Ripper

③ Wireshark

④ Nmap

59. 보안 관리자는 외부 출장 중 사설 와이파이를 사용하는 직원들이 많은 점을 우려하고 있다. 사설 네트워크에서 패킷이 도청(Sniffing)될 가능성을 줄이기 위해 직원들이 회사 내부 서버에 접속할 때 전송 구간 전체를 안전하게 보호할 수 있도록 하려고 한다. 이러한 보안 목적을 달성하기 위한 가장 적절한 접근 방식은?

① 방화벽에서 IP 포트를 변경한다.

② VPN을 통해 사내망과의 연결 구간을 암호화한다.

③ HTTP 대신 FTP를 사용하여 파일을 전송한다.

④ 방화벽 로그를 주기적으로 확인한다.

60. 회사 내부 네트워크에서 사용자의 로그인 정보와 이메일 내용이 외부로 유출되는 사고가 발생했다. 조사 결과, 공격자는 네트워크에 연결된 시스템에서 패킷 분석 도구를 이용해 통신 데이터를 몰래 수집하고 있었던 것으로 확인되었다. 이와 같은 데이터 도청 및 패킷 가로채기 공격 기법을 일컫는 용어는?

① Spoofing

② Sniffing

③ Phishing

④ Spamming