2021년 정보보안기사 필기 기출문제

전 회차 · 54문항 · 정답·해설 포함

출처: 모두CBT(moducbt.com) 공개 기출문제를 연도별·회차별로 정리한 자료입니다.

2021년 정보보안기사 필기

제1회 · 28문항

[1번] 내부 정보 유출 차단을 위한 보안 제품은 무엇인가?

▸ 단말에 에이전트를 설치해 메일·SNS·웹 등 유출 경로를 감시하고 막는 제품은 DLP(Data Loss Prevention)다. DLP는 오가는 데이터의 내용을 키워드·패턴·문서지문으로 검사해 반출 행위 자체를 통제한다. 그래서 메일 전송, 웹 업로드, 출력, 이동식 매체 복사 같은 채널이 모두 감시 대상이 된다. * DRM — 문서를 암호화하고 사용자별 열람·편집 권한을 부여해 유출되더라도 열지 못하게 하는 방식으로, 유출 경로를 탐지·차단하는 것이 목적이 아니다. * VDI — 업무 환경을 중앙 서버의 가상 데스크톱으로 옮겨 자료가 단말에 남지 않게 하는 인프라 방식이다. * EDMS — 전자문서를 등록·결재·보관·검색하는 문서관리 시스템으로 유출 차단 솔루션이 아니다.

[2번] 다음 중 Windows에서 사용하는 일반사용자 그룹인 Users 그룹에 대한 설명 중 적합하지 않은 것은?

1User는 시스템 크기의 레지스트리 설정, 운영체제 파일 또는 프로그램 파일을 수정할 수 없다.
2User는 워크스테이션을 종료할 수는 있지만 서버는 종료할 수 없다.
3Users가 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있다.
4Users 그룹의 구성원은 다른 Users 그룹에서 실행할 수 있는 프로그램을 설치할 수 있다.

▸ Windows의 Users 그룹은 시스템 전반에 영향을 주는 프로그램의 설치나 시스템 파일·레지스트리 변경이 제한되어 있어, 다른 Users가 실행할 수 있는 프로그램이라도 임의로 설치할 수는 없다. 워크스테이션은 종료할 수 있지만 서버는 종료할 수 없다는 점, 자신이 만든 로컬 그룹만 관리할 수 있다는 점은 Users 그룹의 실제 권한 범위와 일치한다.

[3번] 파일 무결성 점검 도구에 해당하는 것은?

1John the Ripper
2Tripwire
3Snort
4Nmap

▸ Tripwire는 파일의 해시값을 주기적으로 비교해 무단 변경 여부를 탐지하는 대표적인 파일 무결성 점검 도구이다. John the Ripper는 패스워드 크래킹 도구, Snort는 침입 탐지 시스템(IDS), Nmap은 포트·서비스 스캐너로 각각 목적이 다르다.

[4번] 주체가 주도적으로 자신이 소유한 객체(파일 등)에 대한 접근권한(Read, Write, Execution, Append 등)을 다른 주체(사용자)에게 양도하는 등의 행위가 가능한 접근통제 정책은?

▸ DAC(임의적 접근통제)는 객체의 소유자가 자신의 판단으로 다른 사용자에게 읽기·쓰기·실행 등의 접근 권한을 부여하거나 양도할 수 있는 방식이다. MAC은 시스템이 정한 보안등급에 따라 강제로 통제되고, RBAC은 역할에 따라, CBAC은 접속 상황(문맥) 조건에 따라 권한이 결정되어 소유자가 임의로 양도할 수 있는 구조가 아니다.

[5번] 다음 지문이 설명하는 파일 시스템은?

1exFAT(Extended File Allocation Table)
2ext4(extended file system)
3HFS(Hierarchical File System)
4ReFS(Resilient File System)

▸ FAT32의 파일 크기·디렉터리 제약을 풀기 위해 마이크로소프트가 만든 파일 시스템은 exFAT이다. exFAT은 윈도우 CE 6.0과 비스타 이후 데스크톱·서버에 도입됐고, 저널링과 보안 기술자 같은 무거운 기능을 덜어내 자료구조 오버헤드를 줄인 구조라 플래시 메모리·SD 카드 등 이동식 대용량 매체에 주로 쓰인다. * ext4 — 리눅스 계열에서 쓰는 파일 시스템으로 마이크로소프트가 만든 것이 아니다. * HFS — 애플 매킨토시에서 쓰던 계층적 파일 시스템이다. * ReFS — 마

이크로소프트 제품이지만 윈도우 서버 2012에서 NTFS를 대체할 복원력 중심으로 도입됐고, 지문이 말하는 도입 시점·대상 제품과 맞지 않는다.

[6번] 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

1바-다-라-가-마-나
2나-바-가-다-라-마
3나-바-다-라-가-마
4바-가-마-나-다-라

▸ 전원을 켠 뒤 진행 순서는 POST → CMOS → MBR → NTLDR → NTDETECT.com → ntoskrnl.exe다. 먼저 펌웨어가 하드웨어 이상 유무를 점검하고(POST), 사용자가 저장해 둔 설정값을 CMOS에서 읽어 적용한다. 그다음 부팅 매체의 첫 섹터인 MBR을 읽어 부팅 파티션의 위치를 알아낸다. 이어 부팅 파티션의 NTLDR이 boot.ini를 읽어 올릴 운영체제를 정하고, NTDETECT.com이 설치된 하드웨어를 조사한 뒤, 마지막으로 커널인 ntoskrnl.exe가 HAL.dll과 함께 적재된다. 하드웨어 점검보다 MBR 읽기가 앞서거나 커널 적재가 하드웨어 검사보다 먼저인 배열은 성립하지 않는다.

[7번] 소유자 외에는 읽기, 쓰기, 실행 등 일체의 접근을 불허하기 위한 umask 설정값으로 알맞은 것은?

1umask 077
2umask 020
3umask 022
4umask 066

▸ umask 077은 소유자 권한을 제외한 그룹과 기타 사용자의 읽기·쓰기·실행 권한을 모두 차단한다. 077은 그룹과 기타 사용자 권한 비트를 모두 마스크하므로 소유자만 접근할 수 있으며, 020·022·066은 일부 권한이 허용될 수 있다.

[8번] 'last' 명령을 사용하여 정보를 확인할 수 있는 로그파일은?

▸ wtmp 파일은 사용자의 로그인·로그아웃 이력을 누적 기록하며, last 명령은 이 파일을 읽어 로그인 기록을 출력한다. utmp는 현재 로그인 중인 세션 정보, pacct는 실행된 명령의 프로세스 회계 정보, lastlog는 사용자별 마지막 로그인 시각을 담고 있어 각각 다른 명령으로 조회한다.

[9번] 다음 지문에서 설명하는 파일은 무엇인가?

1hosts.equiv
2hosts
3inetd.conf
4shadow

▸ IP 주소와 호스트 이름을 직접 대응시켜 두는 /etc/hosts에 대한 설명이다. 이름 해석은 일반적으로 hosts 파일을 DNS보다 먼저 참조하므로, 공격자가 이 파일에 한 줄만 추가해도 정상 도메인이 악성 IP로 연결되는 파밍이 성립한다. 그래서 소유자를 root로 두고 일반 사용자에게 쓰기 권한을 주지 않는 것이 기본 대응이다. * hosts.equiv — 신뢰할 호스트와 사용자를 등록해 r 계열 명령의 인증을 생략시키는 파일로, 이름과 IP를 매핑하지 않는다. * inetd.conf — 슈퍼데몬이 어떤 포트에 어떤 서비스를 띄울지 정의하는 설정 파일이다. * shadow — 계정의 암호화된 패스워드와 만료 정책을 담는 파일이다.

[10번] 다음 지문에서 설명하는 것은?

1Session
2Web Beacon
3Super Cookie
4History Stealing

▸ 지문이 설명하는 것은 웹 비콘(Web Beacon)이다. 쿠키와 결합해 웹사이트 이용·이메일 열람 행동을 추적하려고 페이지나 메일 본문에 심어 두는 1픽셀*1픽셀 크기의 눈에 띄지 않는 임베딩 이미지이며, Web bug·pixel tag·e-mail 트래킹이라는 별칭이 붙는다는 점이 결정적 단서다. * 세션은 서버가 접속 상태를 유지하려고 관리하는 연결 단위일 뿐 추적용 이미지가 아니다. * 슈퍼 쿠키는 일반 쿠키를 지워도 되살아나는 영속형 추적 저장 방식이고, 히스토리 스틸링은 방문 기록 링크의 렌더링 차이를 이용해 방문 사이트 목록을 캐내는 공격 기법이다.

[11번] access log에는 referer라는 필드가 존재한다. 이 필드가 의미하는 것은?

1서비스에서 발생하는 이벤트 서버와 글로벌 카달로그 사이의 연결문제를 기록한다.
2사이트를 방문한 사용자가 어떤 경로를 통해 사이트를 방문했는지 알 수 있게 해준다.
3시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드되지 않는 경우와 같이 구성요소의 오류를 기록한다.
4응용프로그램이 기록한 다양한 이벤트가 저장되며, 저장되는 부분은 소프트웨어 개발자에 의해 결정된다.

▸ 웹 access log의 referer 필드는 사용자가 현재 페이지에 접근하기 직전에 머물렀던 이전 페이지(유입 경로)의 주소를 기록한다. 이를 통해 방문자가 어떤 링크나 검색을 거쳐 사이트로 들어왔는지 추적할 수 있으며, 시스템 이벤트나 드라이버 오류, 애플리케이션 이벤트 로그와는 성격이 다르다.

[12번] 루트 사용자 소유로 SUID 권한을 부여한 경우, 이러한 파일로 의심되는 파일을 검색하는 명령어로 알맞은 것은?

1find / -user –perm –1000 -print
2find / -user –perm –2000 -print
3find / -user –perm –3000 -print
4find / -user –perm –4000 -print

▸ SUID(Set User ID) 권한은 8진수 특수 권한 비트 4000으로 표현되며, find 명령에서 -perm -4000 조건으로 루트 소유 SUID 파일을 검색할 수 있다. 1000은 sticky bit, 2000은 SGID, 3000은 SGID와 sticky bit가 함께 설정된 값을 의미해 SUID 검색 목적과는 맞지 않는다.

[13번] Unix 명령($ ls -l)의 실행 결과에 대한 설명으로 가장 옳은 것은?

1파일 aaa에 대한 소유자는 bbb이다.
2파일 bbb에 대한 소유자는 aaa이다.
3파일 ccc에 대한 소유자는 aaa이다.
4파일 aaa에 대한 소유자는 ccc이다.

▸ 출력된 줄에서 파일 이름은 맨 끝의 ccc이고 그 소유자는 aaa이므로, 파일 ccc의 소유자가 aaa라는 설명이 옳다. 표시된 결과는 -rwxr--r-- aaa bbb 98 Aug 7 19:16 ccc 이며, 왼쪽부터 권한 → 소유자 → 그룹 → 크기 → 수정시각 → 파일명 순이다(실제 ls -l 은 권한과 소유자 사이에 링크 수가 한 칸 더 붙는다). 따라서 aaa는 소유자, bbb는 그룹, 98은 파일 크기, ccc는 파일명이다. aaa·bbb·ccc 가 모두 이름처럼 보이지만 파일명은 줄의 마지막 하나뿐이므로, aaa나 bbb를 파일로 보는 설명은 성립하지 않는다.

[14번] Crontab을 이용해 정기적으로 매일 오전 1시에 아파치 웹 서버 로그를 백업하고자 한다. 백업 경로는 /backup/logs/ 이며, 파일 이름은 “log-년월일시분” 형식을 따른다. 정상적으로 작동시키기 위해 Crontab에 등록해야할 값으로 올바른 것은? (파일이름 예시: log-201903210019)

1* * * 1 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'
20 1 * * * cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'
3* * * 0 1 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'
40 1 * * 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date + %Y %m %d %H %M'

▸ crontab 필드는 분 시 일 월 요일 순서이며, 매일 오전 1시에 실행하려면 일·월·요일 자리를 모두 *로 두고 분과 시만 지정한 0 1 * * * 형태로 작성해야 한다. 요일 자리에 0이나 1을 넣으면 특정 요일에만 실행되고, 분·시 자리를 별표로 두면 매분 실행되어 매일 오전 1시 실행이라는 요건을 만족하지 못한다.

[15번] 하드웨어 및 소프트웨어를 탑재한 시스템 요소를 의미하는 것은?

▸ TCB(Trusted Computing Base)는 하드웨어 및 소프트웨어를 포함해 시스템의 보안 정책을 구현하는 모든 보호 메커니즘의 총체를 의미한다. 시스템 내에서 접근통제 등 보안 기능이 실제로 수행되는 신뢰 기반 요소들을 통칭하는 개념으로, EGID(유효 그룹 ID)·PCB(프로세스 제어 블록)·CC(공통평가기준)와는 성격이 다르다.

[16번] 다음 지문에서 설명하고 있는 공격은 무엇인가?

1스펙터
2캐시 포이즈닝
3멜트다운
4미라이

▸ 지문이 가리키는 것은 멜트다운(Meltdown)이다. 멜트다운은 비순차 명령 실행에서 권한 검사가 끝나기 전에 미리 수행된 결과가 CPU 캐시에 흔적으로 남는 점을 악용해, 일반 프로그램이 커널 영역의 데이터를 간접적으로 읽어내게 만드는 취약점이다. * 스펙터는 같은 시기에 공개된 부채널 취약점이지만 분기 예측을 속여 다른 프로세스 영역을 읽는 방식이라 지문의 비순차 실행 검사 우회와 구분된다. * 캐시 포이즈닝은 DNS 등 서버 캐시에 거짓 정보를 주입하는 네트워크 공격이고, 미라이는 IoT 기기를 감염시켜 대규모 DDoS를 일으킨 악성코드다.

[17번] 윈도우 로그는 무엇인가?

1응용 프로그램 로그
2시스템 로그
3보안 로그
4설정 로그

▸ 운영체제 구성요소가 남기는 기록, 즉 시스템 로그에 대한 설명이다. 윈도우 이벤트 뷰어의 시스템 로그에는 운영체제 시작 시점의 이벤트와 장치 드라이버의 로드 성공·실패처럼 OS 자체 구성요소가 발생시킨 항목이 쌓인다. * 응용 프로그램 로그는 OS가 아니라 설치된 프로그램이 남기는 기록이다. * 보안 로그는 로그온 성공·실패와 개체 접근 감사 등 감사 정책에 따른 기록이며, 윈도우 이벤트 로그에 '설정 로그'라는 기본 분류는 없다.

[18번] 파일 공유와 관련된 서비스 포트에 대한 내용으로 적절하지 않은 것은?

1445(TCP/UDP, Direct Host)
2139(TCP, NetBIOS Session)
3137(UDP, NetBIOS Name)
4335(UDP, NetBIOS Datagram)

▸ NetBIOS Datagram Service는 138번 UDP 포트를 사용하므로, 335번이라는 설명은 옳지 않다. 파일 공유(SMB) 환경에서는 445(TCP/UDP), NetBIOS Name(137, UDP), NetBIOS Datagram(138, UDP), NetBIOS Session(139, TCP) 포트가 함께 쓰인다.

[19번] 유닉스 시스템에서 계정과 패스워드에 관련된 설명으로 틀린 것은?

1유닉스 시스템에서 사용자들은 각각 고유의 아이디를 갖고 있으며, 그 아이디에 대한 정보는 /etc/passwd에 저장된다.
2유닉스 시스템에서는 각각의 사용자만이 접근 가능한 파일과 디렉터리가 존재할 수 있다.
3사용자 패스워드는 /etc/passwd 또는 /etc/shadow 파일에서 관리한다.
4/etc/shadow 파일에는 사용자의 패스워드가 AES-256 알고리즘에 의해 암호화되어 저장된다.

▸ 유닉스의 패스워드는 AES-256 같은 대칭키 암호화가 아니라 단방향 해시(crypt, MD5, SHA-512 등)로 변환되어 저장된다. 해시는 복호화가 불가능한 일방향 함수이므로, 암호화되어 저장된다는 설명은 옳지 않다.

[20번] 접근권한을 확인하였더니 'rwSr- -r- -'이었다. 권한 내의 대문자 S에 대한 설명으로 옳은 것은?

1SetUID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
2SetGID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
3디렉터리에 스티키 비트가 설정되어 대문자 S로 표기하였다.
4SetGID를 설정하여 대문자 S로 표기하였다.

▸ SetUID 비트가 설정된 파일에 소유자 실행 권한(x)이 없는 경우 소문자 s 대신 대문자 S로 표기된다. 실행 권한이 있으면 소문자 s로 표기되어, S와 s는 실행 권한 유무를 함께 나타내는 표기 방식이다.

[21번] 다음은 WEP에 대한 설명이다. 빈칸 ㉠에 들어갈 내용으로 적절한 것은?

1Encryption Key
2Initial Key
3Initial Vector
4Encryption Vector

▸ 빈칸에 들어갈 것은 Initial Vector(초기화 벡터, IV)이다. WEP은 RC4 스트림 암호를 쓰기 때문에 같은 비밀키로 같은 키스트림이 반복되면 안 된다. 그래서 프레임마다 랜덤한 24비트 IV를 만들어 비밀키 앞에 붙여 키스트림을 생성하고, 그 IV는 상대가 복호할 수 있도록 평문으로 단말에 함께 전송한다. 지문의 '키 생성 순서 예측 방지를 위해 랜덤하게 생성해 무선 단말기에 보낸다'가 바로 IV의 역할이다. 실제 암·복호에 쓰는 비밀키 자체는 전송되지 않으므로 Encryption Key·Initial Key 처럼 키를 뜻하는 용어는 빈칸에 들어갈 수 없고, Encryption Vector 는 WEP 규격에 없는 용어다.

[22번] 무선랜의 전송 패킷에 덧붙여지는 32bytes 길이의 고유 식별자로서, 무선장치들이 BSS(Basic Service Set)에 접속할 때 패스워드같이 사용되는 코드는 무엇인가?

1무선 네트워크 아이디(SSID)
2WEP(Wired Equivalent Privacy)
3MAC(Message Authentication Code)
4RFID 태그

▸ 무선 패킷에 덧붙는 32바이트 이하의 고유 식별자로 BSS 접속 시 패스워드처럼 쓰이는 것은 SSID(무선 네트워크 식별자)이다. WEP은 암호화 방식, MAC(Message Authentication Code)은 무결성·인증용 코드, RFID 태그는 별도의 무선 식별 기술로 이 설명과는 무관하다.

[23번] 지문에서 설명하고 있는 것은?

1NFV(Network Function Virtualization)
2MDR(Managed Detection & Response)
3EDR(Endpoint Detection & Response)
4SDN(Software Defined Networking)

▸ 지문이 설명하는 것은 SDN(Software Defined Networking)이다. SDN은 네트워크 장비의 제어 평면과 데이터 평면을 분리해 폐쇄적이던 장비를 개방형 인터페이스로 열고, 컨트롤러 소프트웨어가 트래픽 흐름을 직접 제어하게 한다. 그 덕분에 지문처럼 미세흐름 조정, QoS 보장, 손쉬운 장비 관리가 가능해진다. * NFV는 방화벽·로드밸런서 같은 네트워크 기능을 가상 소프트웨어로 구현하는 기술이어서 장비 제어 구조를 개방한다는 설명과 초점이 다르다. * EDR과 MDR은 단말 위협 탐지·대응과 그 관제 서비스여서 네트워크 구조의 패러다임과는 무관하다.

[24번] 다음 중 지능형 지속 위협에 대한 설명으로 옳은 것은?

1공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.
2다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.
3시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.
4하나의 타깃에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

▸ 지능형 지속 위협(APT)은 특정 대상을 겨냥해 다양한 침투 경로를 장기간 시도하므로, 방어자는 가능한 모든 공격 경로를 대비해야 해 방어가 매우 어렵다. 공격 설계부터 침투까지 오랜 시간과 많은 비용이 들고, 하나의 방법만 반복하기보다 여러 기법을 병행한다는 점에서 다른 설명들과 구분된다.

[25번] 다음 지문의 빈칸 ㉠, ㉡에 들어갈 용어로 올바르게 짝지어진 것은?

1㉠ MAC ㉡ 암호화
2㉠ MAC ㉡ 인증
3㉠ 스위치 ㉡ 인증
4㉠ 스위치 ㉡ 암호화

▸ ㉠에는 MAC, ㉡에는 암호화가 들어간다. 랜카드를 무차별 모드(promiscuous mode)로 두면 목적지 MAC 주소가 자기 것이 아닌 프레임도 버리지 않고 상위 계층으로 올려 스니핑이 가능해진다. 랜카드가 프레임을 걸러내는 기준이 MAC 주소이기 때문이다. 스니핑은 엿듣는 행위 자체를 막기 어려우므로, 가로채더라도 내용을 알아볼 수 없게 만드는 통신 구간 암호화가 가장 효과적인 대응이다. 스위치 환경은 ARP 스푸핑 등으로 우회되고, 인증은 접속 자격만 확인할 뿐 오가는 내용을 보호하지 못한다.

[26번] OSI 7 Layer 중 어느 계층에 대한 설명인가?

1Transport Layer
2Network Layer
3Session Layer
4Physical Layer

▸ 데이터 유실 없이 End-to-End 신뢰성을 보장하고 오류가 있으면 재전송을 요구하는 계층은 전송 계층(Transport Layer)이다. 전송 계층은 종단 프로세스 사이에서 순서 제어·흐름 제어·오류 제어와 재전송을 담당하며, TCP가 바로 이 기능을 수행한다. * 네트워크 계층은 라우팅과 논리 주소 지정을 맡을 뿐 전달을 보장하지 않는다. * 세션 계층은 통신 연결의 설정·유지·동기점 관리를, 물리 계층은 비트의 전기적 전송을 담당한다.

[27번] 1출발지 211.1.99.1 / 목적지주소 32.15.1.1인 패킷은 규칙 1에 의해 거부된다.

2출발지 211.1.99.1 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.
3출발지 211.1.37.15 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.
4출발지 211.1.37.15 / 목적지주소 32.15.1.1인 패킷은 규칙 3에 의해 차단된다.

▸ 이 문항은 원본 출처에서 문제 또는 보기 내용이 정확하지 않다고 밝힌 문항입니다. 지문이 원래 시험 문제와 다를 수 있으니 개념 확인용으로만 활용하시기 바랍니다.

[28번] TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?

1CLOSED→SYN_RCVD→ESTABLISHED
2CLOSED→SYN_SENT→ESTABLISHED
3LISTEN→SYN_RCVD→ESTABLISHED
4LISTEN→SYN_SENT→ESTABLISHED

▸ 클라이언트는 연결을 시작할 때 CLOSED 상태에서 SYN을 보내 SYN_SENT로 전이하고, 서버의 SYN+ACK에 ACK로 응답한 뒤 ESTABLISHED 상태가 된다. SYN_RCVD와 LISTEN은 서 </partial_content> <instructions> Document is too large (77409 tokens). Only showing first 10000 tokens. For complete analysis, run `gsk summarize "https://www.moducbt.com/exam/pdf/28434" --question "<your specific question>"` — it analyzes the full document (PDFs, academic pape

제2회 · 26문항

[1번] NTFS 파일 시스템의 메타 데이터 해당하지 않는 것은?

1$MFT
2$Logfile
3$Volume
4$Bios

▸ $Bios는 NTFS의 메타데이터 파일이 아니다. NTFS는 $MFT, $LogFile, $Volume 외에도 $Bitmap, $Boot, $Secure 등 $로 시작하는 시스템 파일들로 메타데이터를 관리하는데, 이 중 $Bios라는 항목은 존재하지 않는다.

[2번] 다음 지문에서 설명하는 공격은 무엇인가?

1힙 오버플로우 공격
2레이스 컨디션 공격
3스택 오버플로우 공격
4코드 기반 공격

▸ 두 프로세스가 같은 자원을 두고 경쟁 상태(Race Condition)에 놓이는 순간을 노려 SetUID 프로그램의 권한을 가로채는 공격이다. SetUID가 걸린 프로그램이 파일 존재를 확인한 뒤 실제로 그 파일을 여는 사이의 짧은 시간 틈에 공격자가 해당 경로를 심볼릭 링크로 바꿔치기하면, 프로그램은 root 권한으로 공격자가 지정한 파일을 열거나 덮어쓰게 된다. * 스택 오버플로우: 지역변수 버퍼를 넘치게 해 스택의 복귀주소를 덮는 공격 * 힙 오버플로우: 동적 할당 영역을 넘치게 해 관리 구조나 함수 포인터를 조작하는 공격 이 둘은 모두 버퍼 경계 검사 부재를 노린 메모리 손상 공격이어서, 두 프로세스의 실행 순서 차이를 이용하는 지문의 설명과 다르다.

[3번] 리눅스에서 새로 생성되는 사용자 계정의 홈 디렉터리는 .bashrc 등과 같이 모든 사용자가 필요로 하는 파일들을 만들어줄 필요가 있다. 이러한 공통 파일들을 미리 만들어 특정 디렉터리에 넣어두면 사용자 계정 생성 시 자동복사 되도록 설정할 수 있는데, 이러한 용도의 디렉터리는 무엇인가?

1/etc/init
2/etc/services
3/etc/login.defs
4/etc/skel

▸ 리눅스에서 신규 사용자 계정 생성 시 홈 디렉터리에 기본으로 복사되는 공통 파일들을 모아두는 곳은 /etc/skel이다. useradd로 계정을 만들면 /etc/skel 안의 .bashrc, .profile 등의 파일이 새 홈 디렉터리로 자동 복사된다. * /etc/init은 시

스템 초기화 스크립트 디렉터리다. * /etc/services는 포트와 서비스명 매핑 파일이다. * /etc/login.defs는 계정 정책(UID 범위, 비밀번호 만료 등) 설정 파일이다.

[4번] 2016년에 처음 발견되었으며 IP 카메라나 가정용 라우터와 같은 IoT 장치를 주요 공격 대상으로 삼는 DDoS 공격용 봇넷 악성코드는 무엇인가?

1님다
2미라이
3스턱스넷
4SQL 슬래머

▸ 2016년 처음 발견되어 IP 카메라·홈라우터 등 IoT 장치를 감염시켜 대규모 DDoS에 악용된 봇넷은 미라이(Mirai)다. 미라이는 기본 계정·비밀번호가 바뀌지 않은 IoT 장치를 스캔해 감염시키고, 감염된 다수의 장치로 봇넷을 구성해 목표 서버에 트래픽을 집중시키는 방식으로 동작한다.

[5번] 다음 지문에서 설명하는 내용은 스푸핑 공격 중 어떤 공격에 해당하는가?

32bit IP 주소를 48bit의 네트워크 카드 주소(MAC Address)로 대응시켜 주는 프로토콜이고 실제로 IP 주소를 통해 네트워크 연결을 시도하면 TCP/IP에서는 해당 IP주소 해당하는 네트워크 카드 주소를 찾아 연결하게 된다. 이더넷 환경에서 공격대상자의 cache 테이블에 공격자가 원하는 IP에 대한 하드웨어 주소(MAC Address)를 거짓으로 지정하여 업데이트함으로써 공격대상자의 패킷 흐름을 공격자가 원하는 방향으로 조절하여 공격하는 기술이다.
1DHCP 스푸핑
2IP 스푸핑
3DNS 스푸핑
4ARP 스푸핑

▸ 32비트 IP 주소를 48비트 MAC 주소로 대응시키는 프로토콜의 캐시를 거짓 정보로 갱신하는 공격이므로 ARP 스푸핑이다. ARP는 요청을 보낸 적이 있는지조차 검증하지 않고 받은 응답으로 캐시를 갱신하기 때문에, 공격자가 위조 ARP 응답을 지속적으로 보내면 피해자의 ARP 캐시에 공격자 MAC이 등록되어 같은 이더넷 세그먼트의 트래픽이 공격자를 거쳐 흐르게 된다. * IP 스푸핑: 패킷의 출발지 IP를 위조해 신뢰관계를 악용하는 공격으로 MAC 캐시와 무관하다 * DNS 스푸핑: 도메인 질의에 가짜 응답을 먼저 보내 다른 IP로 유도하는 공격이다 * DHCP 스푸핑: 가짜 DHCP 서버를 띄워 IP·게이트웨이·DNS 정보를 잘못 할당하는 공격이다

[6번] 디지털저장매체 중 하드디스크 구조에서 물리적으로는 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 무엇이라고 하는가?

1슬랙
2CHS
3클러스터
4확장 공간

▸ 디스크에서 물리적으로는 클러스터가 할당되어 있지만 실제 파일 크기가 그보다 작아 논리적으로 사용할 수 없는 여유 공간을 슬랙(Slack) 공간이라 한다. 이 영역은 이전에 저장되어 있던 데이터의 잔재가 남아 있을 수 있어 디지털 포렌식에서 중요한 증거 수집 대상이 된다.

[7번] 윈도우 레지스트리 키 중에서 파일의 각 확장자에 대한 정보와 프로그램의 맵핑 정보가 저장된 키로 옳은 것은?

1HKEY_CLASSES_ROOT
2HKEY_CURRENT_USER
3HKEY_FILE_EXT
4HKEY_LOCAL_MACHINE

▸ 파일 확장자별 프로그램 연결 정보(파일 형식-프로그램 매핑, COM 등록 정보)가 저장되는 레지스트리 키는 HKEY_CLASSES_ROOT다. HKEY_CURRENT_USER는 로그인한 사용자별 설정, HKEY_LOCAL_MACHINE은 시스템 전역 설정을 담고 있어 확장자 연결 정보와는 다르며, HKEY_FILE_EXT라는 키는 존재하지 않는다.

[8번] 다음 지문에서 설명하고 있는 시스템 보안은?

▸ 민감한 암호 연산을 전용 하드웨어 칩으로 옮겨 안전한 부팅과 키 보관을 제공하는 것은 TPM(Trusted Platform Module)이다. TPM은 메인보드에 탑재되는 암호 프로세서로, 부팅 단계마다 무결성 측정값을 저장해 인증된 부트를 보장하고 암호키를 칩 내부에 봉인해 소프트웨어 공격으로 유출되지 않게 한다. * SRM: 윈도우 커널에서 객체 접근 권한을 판단하는 보안 참조 모니터로 소프트웨어 구성요소다 * SAM: 윈도우 계정과 패스워드 해시를 저장하는 데이터베이스다 * SID: 사용자·그룹을 구분하기 위한 보안 식별자 값이다

[9번] 아래 지문의 척도들과 가장 관련성이 높은 보안 서비스는?

1기밀성
2무결성
3가용성
4유지보수성

▸ 가동시간과 정지시간, MTTF·MTTR은 시스템을 필요할 때 쓸 수 있는 정도를 재는 지표이므로 가용성과 직결된다. 가용성은 보통 가동시간 ÷ (가동시간 + 정지시간)으로 계산하며, 장애 발생까지의 평균 시간(MTTF)이 길고 복구에 걸리는 평균 시간(MTTR)이 짧을수록 높아진다. * 기밀성: 인가되지 않은 대상에게 정보가 노출되지 않는 성질로 암호화·접근통제로 확보한다 * 무결성: 정보가 위·변조되지 않은 성질로 해시·전자서명으로 확인한다 * 유지보수성: 고치기 쉬운 정도를 뜻하는 품질 속성이며 정보보호의 3대 요소에 들지 않는다

[10번] IoT 위협 및 보안에 대한 설명으로 올바르지 않은 것은?

1홈가전 IoT 제품의 보안 요구사항에는 시큐어 코딩, 알려진 보안약점 및 취약점 제거, 최신 제3자(3rd party) 소프트웨어 사용 등이 있다.
2홈캠, 네트워크 카메라 등의 네트워크 제품에 대한 주요 보안 위협에는 사진 및 동영상을 공격자의 서버 및 이메일로 전송하는 것이 있다. 이에 대한 원인으로는 접근통제 및 전송 데이터 보호의 부재가 있다.
3시큐어 코딩이 적용되지 않은 스마트 홈가전 제품의 경우 입력 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러처리 등에서 보안 취약점이 발생할 수 있다.
4스마트 홈가전 제품의 데이터 기밀성 및 무결성을 위해 안전한 암호인 MD5, SHA-1 등의 사용이 권장된다.

▸ 스마트 홈가전의 데이터 기밀성·무결성을 위해 MD5, SHA-1 사용을 권장한다는 설명이 옳지 않다. MD5와 SHA-1은 이미 충돌 공격이 실증되어 취약성이 드러난 알고리즘으로, 오늘날에는 SHA-256 이상의 안전한 해시 알고리즘 사용이 권장된다. 나머지 보기는 시큐어 코딩·접근통제·전송데이터 보호 등 IoT 보안 위협과 대응에 대한 올바른 설명이다.

[11번] 기존 파일 시스템에 새로운 파일 시스템을 하위 디렉터리로 연결하기 위해 사용하는 명령어는 무엇인가?

▸ 기존 파일 시스템에 새 파일 시스템을 특정 디렉터리에 연결해 사용할 수 있게 하는 명령어는 mount다. * mkfs는 새 파일 시스템을 생성(포맷)하는 명령어다. * fsck는 파일 시스템의 무결성을 점검·복구하는 명령어다. * mknod는 특수 파일(장치 파일 등)을 생성하는 명령어다.

[12번] 유닉스에서는 패스워드 보호를 위해 암호 처리된 패스워드 정보를 공격자가 접근하기 어렵게 일반 사용자 권한으로 접근할 수 없는 (㉠)를 사용하고 있다.

1해시 암호화 패스워드 파일
2섀도(Shadow) 패스워드 파일
3익명(Anonymity) 패스워드 파일
4PAM(Pluggable Authentication Module) 패스워드 파일

▸ 암호화된 패스워드를 일반 사용자가 읽지 못하도록 따로 떼어 둔 것은 섀도(Shadow) 패스워드 파일이다. 원래 /etc/passwd는 모든 사용자가 읽을 수 있어 해시가 그대로 노출됐는데, 해시를 /etc/shadow로 옮기고 root만 읽을 수 있게 권한을 제한해 사전 공격이나 무차별 크래킹 시도를 차단한다. * 해시 암호화 자체는 passwd 파일에서도 이미 쓰이던 방식이라 접근 권한을 제한한다는 설명과 맞지 않는다 * PAM은 인증 방식을 모듈로 끼워 넣는 인증 프레임워크이지 패스워드를 저장하는 파일이 아니다

[13번] [그림1]은 어떤 리눅스 시스템에 존재하는 특정 /home 디렉터리와 그 아래에 존재하는 디렉터리 및 파일들의 속성 중 name, permission, user, group 등에 대한 정보만 요약한 것이며, [그림2]는 이 시스템에 존재하는 /etc/group 파일의 일부분이다. 이를 통하여 확인할 수 있는 파일 및 디렉터리의 permission에 관한 설명 중 올바르지 않은 것은?

1user1이란 사용자는 /home/user1 디렉터리로 이동할 수 있다

2user2란 사용자는 exam.txt란 파일의 내용을 읽을 수 있다.
3user3란 사용자는 exam.txt란 파일을 삭제할 수 있다.
4시스템 내에 존재하는 user4란 사용자는 /home/user1 디렉터리로 이동할 수 없다.

▸ 파일을 지우려면 그 파일이 들어 있는 디렉터리에 쓰기(w) 권한이 있어야 하는데, security 그룹인 user3에게 /home/user1은 drwxr-x---로 r와 x만 허용되므로 exam.txt를 삭제할 수 없다. 삭제는 파일 자체의 rw- 권한이 아니라 디렉터리 안의 파일 목록을 고치는 작업이라는 점이 판단의 기준이다. * user1은 /home/user1의 소유자로 rwx를 가지므로 그 디렉터리로 이동할 수 있다 * user2는 /etc/group에서 security 그룹원이므로 /home/user1에 x가 있어 들어갈 수 있고, exam.txt의 그룹 권한 rw로 내용을 읽을 수 있다 * user4는 security 그룹에 없어 기타 사용자 권한(---)만 적용되므로 /home/user

[14번] 다른 로그파일에 비해 많은 정보를 포함하고 있는 로그파일로 동작 중인 서비스에 대한 버퍼 오버플로우 공격의 경우와 같이 시스템 장애에 대한 정보를 로그파일로 저장한다.

1btmp
2wtmp
3syslog
4messages

▸ 시스템 전반의 장애·오류 메시지가 가장 폭넓게 남는 로그는 messages 로그다. 커널과 각종 데몬이 syslog 체계를 통해 보낸 메시지가 이곳에 모이므로, 서비스 비정상 종료나 버퍼 오버플로우로 인한 세그먼테이션 폴트 같은 장애 흔적을 여기서 확인한다. * btmp: 로그인 실패 기록만 남기는 바이너리 로그다 * wtmp: 로그인·로그아웃과 재부팅 이력을 남기는 바이너리 로그다 * syslog: 로그를 수집·분배하는 로깅 체계를 가리키는 이름으로, 시스템 장애 정보를 폭넓게 담는 텍스트 로그의 대표로는 보지 않는다

[15번] 랜섬웨어에 해당하지 않는 것은?

1페트야(Petya)
2크립토월(CryptoWall)
3워너크라이(WannaCry)
4크립토재커(CryptoJacker)

▸ 크립토재커(CryptoJacker)는 시스템 자원을 몰래 이용해 암호화폐를 채굴하는 크립토재킹(가상화폐 무단 채굴) 악성코드로, 파일을 암호화해 금전을 요구하는 랜섬웨어와는 목적과 동작 방식이 다르다. 페트야, 크립토월, 워너크라이는 모두 파일을 암호화한 뒤 복호화 대가로 금전을 요구하는 대표적인 랜섬웨어다.

[16번] 서버의 파일 시스템에 대한 시간 속성이 잘못 기술된 것은?

1mtime: 파일을 생성하거나 내용을 수정한 시간
2atime: 최근 파일을 읽거나 실행시킨 시간
3ctime: 파일 속성이 변경된 시간
4rtime: 파일을 실시간 실행시킨 시간

▸ rtime이라는 파일 시간 속성은 존재하지 않으므로 이 설명이 옳지 않다. 일반적으로 파일 시스템은 mtime(수정시간), atime(접근시간), ctime(속성 변경시간)의 세 가지를 기본으로 관리하며, 이를 흔히 MAC 타임이라 부른다.

[17번] 다음에서 설명하고 있는 것은 무엇인가?

1sudo
2PAM
3Batch file
4Shell script

▸ 설명하는 것은 PAM(Pluggable Authentication Module)이다. 인증 절차를 응용프로그램 본체에서 떼어내 공유 라이브러리 묶음으로 제공하는 리눅스의 인증 프레임워크다. 덕분에 login·su·ftp 같은 프로그램을 재컴파일하지 않고 /etc/pam.d 의 설정 파일만 바꿔 비밀번호·LDAP·생체인증 등으로 인증방식을 갈아끼울 수 있다. * sudo: 일반 사용자가 관리자 권한으로 명령을 실행하도록 하는 권한 위임 도구로, 인증 방식 자체를 교체하는 라이브러리가 아니다. * Batch file·Shell script: 명령을 모아 실행하는 스크립트 파일일 뿐 인증 모듈 구조와 무관하다.

[18번] 윈도우 NTFS 파일 시스템의 특징으로 옳지 않은 것은?

1파일과 폴더에 개별 권한을 설정할 수 있어 강력한 보안정책 설정이 가능하다.
2이벤트 뷰어를 사용하여 MFT(Master File Table)의 내용을 확인할 수 있다.
3FAT 파일 시스템에 없는 보안 속성(사용자 접근제어) 정보를 내장하고 있다.
4파일 압축 및 암호화를 위한 구조를 갖는다.

▸ 윈도우의 이벤트 뷰어는 응용 프로그램·보안·시스템 등의 이벤트 로그를 확인하는 도구일 뿐, MFT(Master File Table) 내용을 확인하는 용도가 아니므로 이 설명이 옳지 않다. MFT는 NTFS가 각 파일·폴더의 메타데이터를 기록해 두는 구조로, 그 내용을 보려면 포렌식 도구 등 별도의 분석 도구가 필요하다. 나머지 보기는 개별 권한 설정, 사용자 접근제어 속성, 압축·암호화 구조 등 NTFS의 실제 특징을 올바르게 설명하고 있다.

[19번] rlogin 접속을 허용하는 설정 파일들로 올바르게 짝지어진 것은?

1/etc/hosts.allow, /etc/exports
2/etc/hosts.allow, /.rhosts
3/etc/hosts.equiv, /etc/exports
4/etc/hosts.equiv, /.rhosts

▸ rlogin 접속을 신뢰 관계로 허용하는 설정 파일은 시스템 전체 신뢰 목록인 /etc/hosts.equiv와 사용자별 신뢰 목록인 /.rhosts다. 두 파일에 등록된 호스트·사용자는 비밀번호 없이 rlogin/rsh 접속이 허용되므로 관리가 소홀하면 심각한 보안 위협이 된다. /etc/hosts.allow는 TCP 래퍼 접근제어용, /etc/exports는 NFS 공유 설정용 파일로 rlogin 신뢰 관계와는 무관하다.

[20번] 다음 지문에서 설명하고 있는 안전한 보안 인증 방식은?

1SSH(Secure Shell)
2SAM(Secure Access Module)
3SSO(Single Sign On)
4PAM(Pluggable Authentication Module)

▸ 지문이 가리키는 것은 PAM(Pluggable Authentication Module)이다. 인증 기능을 끼워 넣을 수 있는(pluggable) 모듈로 분리해 공유 라이브러리 형태로 제공한다. 응용 프로그램은 인증 코드를 직접 갖지 않고 이 라이브러리를 호출하므로, 시스템 환경에 맞춰 설정만 바꾸면 여러 인증 방식을 부가적으로 조합할 수 있다. * SSH(Secure Shell): 원격 접속 구간을 암호화하는 통신 프로토콜이지 인증 모듈 라이브러리가 아니다. * SAM(Secure Access Module): 단말에 탑재해 키를 보관·연산하는 보안 모듈로, OS 의 인증 프레임워크와 성격이 다르다. * SSO(Single Sign On): 한 번 인증으로 여러 서비스를 이용하는 통합 인증 개념이라

[21번] ㉠에 들어갈 용어로 적절한 것은?

1Duplex Mode
2MAC 변조
3Promiscuous Mode
4ARP

▸ ㉠ 에 들어갈 말은 Promiscuous Mode(무차별 모드)다. NIC 는 평소 자기 MAC 주소 앞으로 온 프레임과 브로드캐스트만 상위로 올리는데, 스니핑을 하려면 목적지가 자신이 아닌 프레임까지 전부 받아들이는 무차별 모드로 바꿔야 한다. 그래서 탐지 도구는 각 호스트 NIC 가 이 모드인지를 검사한다. * Duplex Mode: 송수신을 동시에 할지(전이중/반이중)를 정하는 통신 방식 설정으로 패킷 수집 여부와 무관하다. * MAC 변조: 주소를 속이는 공격 기법이지 NIC 의 수신 모드 상태를 가리키지 않는다. * ARP: IP 주소를 MAC 주소로 변환하는 프로토콜로, 스푸핑에 악용될 뿐 NIC 모드가 아니다.

[22번] 다음 지문에서 설명하는 공격 대응 방법은 무엇인가?

1DNS 라우팅
2DNS 스푸핑
3DNS 웜홀
4DNS 싱크홀

▸ 설명하는 대응 방법은 DNS 싱크홀(DNS Sinkhole)이다. 악성봇이 명령·제어(C&C) 서버 도메인을 질의하면 DNS 가 진짜 IP 대신 싱크홀 서버 주소를 응답해 연결을 돌려버린다. 그 결과 감염 PC 는 해커의 악의적인 명령을 전달받지 못하고, 관리자는 싱크홀에 접속해 온 IP 로 감염 단말을 찾아낼 수 있다. * DNS 스푸핑: 거짓 응답을 보내 사용자를 악성 사이트로 유도하는 공격 기법이므로 대응 방법이 될 수 없다. * DNS 라우팅·DNS 웜홀: 악성봇 차단 대응책으로 통용되는

기술 용어가 아니다.

[23번] Firewall, IDS, IPS의 비교 중 올바른 것으로 짝지어진 것은?

1㉠, ㉢
2㉡, ㉢
3㉠, ㉣, ㉤
4㉠, ㉢, ㉣

▸ 표에서 바르게 적힌 줄은 패킷 차단·이상 탐지·장점 세 항목이다. 패킷 차단은 방화벽과 IPS 가 수행하고 IDS 는 탐지·경보만 하므로 표의 ○×가 맞고, 이상 탐지는 IDS 와 IPS 가 함께 갖는 기능이라 역시 맞다. 장점도 방화벽은 엄격한 접근 통제, IDS 는 실시간 탐지, IPS 는 세션 기반 탐지로 통용되는 설명이다. * 오용 탐지 줄: 시그니처로 알려진 공격을 잡는 오용 탐지는 IDS 의 대표 방식인데 표에는 ×로 되어 있어 틀렸다. * 단점 줄: 방화벽의 약점은 허용 정책을 통과한 트래픽과 내부에서 발생하는 공격에 취약하다는 점이므로 "외부 공격에 취약"은 맞지 않다.

[24번] 다음 지문에서 설명하는 용어는 무엇인가?

1HSM
2비트라커
3OTP
4TCB

▸ 설명하는 장치는 HSM(Hardware Security Module)이다. 암호화·복호화·전자서명 연산을 전용 칩으로 고속 처리하고, 암호키를 장치 내부에서 생성해 외부로 추출되지 않게 보관하는 것이 핵심이다. 물리적 변조를 감지하면 키를 스스로 파기하는 내변조성도 갖춘다. * 비트라커: 윈도우의 디스크 전체 암호화 소프트웨어 기능으로, 연산 가속과 키 보관을 담당하는 하드웨어 장치가 아니다. * OTP: 일회용 비밀번호를 생성해 사용자를 인증하는 수단이라 역할이 다르다. * TCB: 보안 정책을 집행하는 하드웨어·소프트웨어·펌웨어 전체를 가리키는 신뢰 컴퓨팅 기반 개념이다.

[25번] 침입차단시스템에 대한 설명으로 옳지 않은 것은?

1패킷 필터링 방화벽은 패킷의 통과여부를 결정하기 위해 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 등을 이용한다.
2응용 게이트웨이 방식 방화벽은 내부망으로 패킷이 전송되는 것을 방지할 수 있으며 사용자 인증 기능도 제공할 수 있다.
3상태 기반 패킷 검사(SPI) 방식 방화벽은 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 외에 패킷의 데이터 부분에 대한 점검도 수행하지만, nmap 도구에 의해 ACK 스캔을 차단하지 못하는 단점이 있다.
4심층 패킷 분석(DPI) 방식 방화벽은 패킷의 데이터 부분에 포함된 바이러스 등 악성코드를 검사할 수 있다.

▸ 상태 기반 패킷 검사(SPI) 방식 방화벽에 대한 설명이 옳지 않다. SPI는 연결의 상태(세션) 정보를 추적해 패킷 통과 여부를 판단하는 방식으로, 패킷의 데이터 부분(payload)까지 검사하는 것은 SPI가 아니라 심층 패킷 분석(DPI)의 역할이다. 또한 SPI는 세션 상태를 추적하기 때문에 정상 연결 없이 들어오는 ACK 패킷(예: nmap의 ACK 스캔)을 비정상으로 판단해 차단할 수 있어, 차단하지 못한다는 설명도 사실과 다르다.

[26번] 서비스의 가용성과 성능뿐만 아니라 DDoS 공격 대응에도 효과적이서 최근 Anycast DNS가 많이 도입되어 있다. 다음 중 이 기술에 대해 잘못 설명한 것은?

1사용자가 접속에 사용하는 IP 주소의 패킷은 해당 주소를 갖는 가장 가까운 호스트로 라우팅된다.
2주요 라우팅 프로토콜로 OSPF가 사용된다.
3IPv4/IPv6 anycast 모두 적용 가능하다.
41.1.1.1이나 8.8.8.8