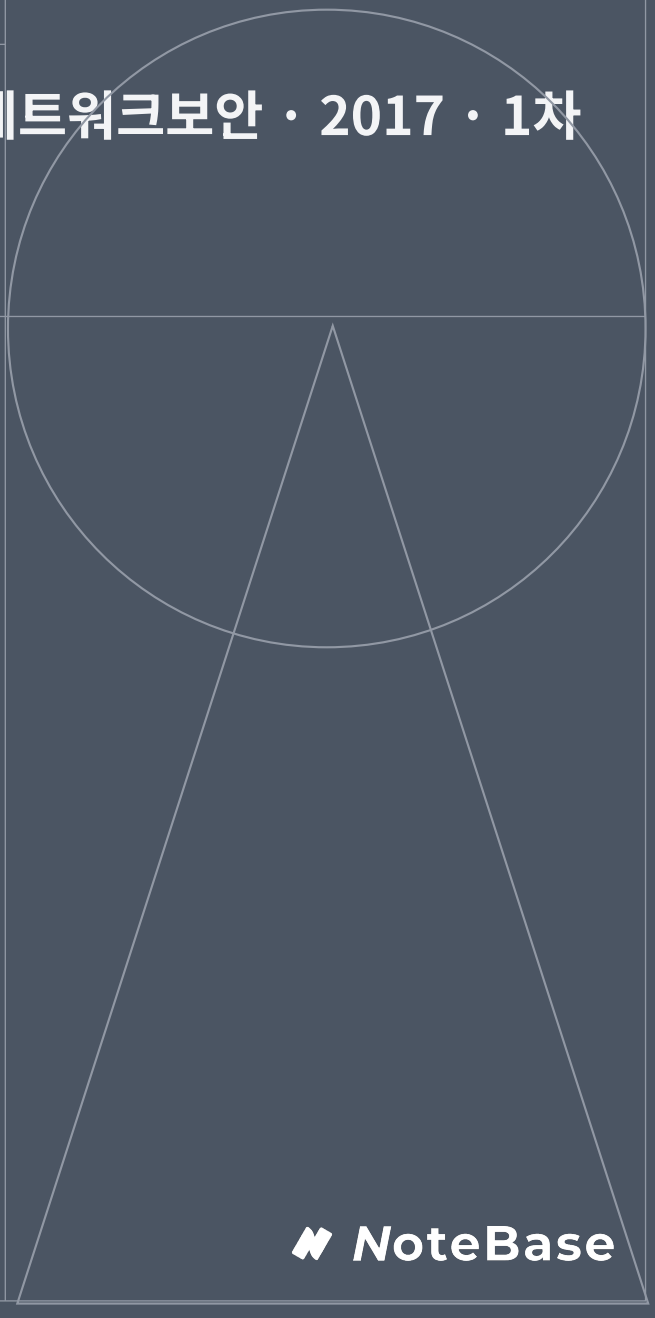
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2017 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2017 · 1차

공무원/해경/일반직 9급 · 네트워크보안 · 2017 · 1차

문 1. 다음에서 설명하고 있는 네트워크 공격은 무엇인가?

· ICMP의 echo 패킷을 이용하여 reply 패킷의 폭주를 통해 시스템을 마비시킨다.
· 공격자는 ping의 목표주소를 네트워크 브로드캐스트 주소로 할당하고 자신을 공격할 호스트로 위장한 후 echo 패킷을 전송한다.

① Teardrop 공격
② UDP flooding 공격
③ Smurf 공격
④ ICMP redirection 공격

정답 3번

출제 포인트

ICMP Echo Request를 브로드캐스트 주소로 보내고 출발지 주소를 피해자의 주소로 위조하여 다수의 Echo Reply가 피해자에게 집중되게 하는 Smurf 공격의 특징을 묻는 문제이다.

핵심 개념

Smurf 공격은 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 네트워크의 브로드캐스트 주소로 보내, 여러 호스트의 Echo Reply가 피해자에게 몰리게 하는 반사·증폭형 서비스 거부 공격이다. Teardrop은 서로 겹치거나 비정상적인 IP 단편을 이용하고, UDP flooding은 대량의 UDP 패킷을 직접 전송하며, ICMP redirection은 위조된 ICMP Redirect 메시지로 호스트의 경로 선택을 바꾸려는 공격이다.

NoteBase

선지별 해설

① X
'Teardrop 공격'이 틀린 표현이다. Teardrop 공격은 겹치거나 비정상적인 IP 단편을 보내 수신 시스템의 재조립 과정에 오류를 일으키는 공격이다. 제시문의 공격은 올바르게는 Smurf 공격이다.

② X
'UDP flooding 공격'이 틀린 표현이다. UDP flooding 공격은 대량의 UDP 패킷을 보내 대역폭이나 시스템 자원을 고갈시키는 공격이다. 제시문의 공격은 올바르게는 Smurf 공격이다.

③ O
Smurf 공격은 피해자의 IP 주소로 출발지를 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 Echo Reply가 피해자에게 집중되게 한다. 제시문의 두 특징과 모두 일치한다.

④ X
'ICMP redirection 공격'이 틀린 표현이다. ICMP redirection 공격은 위조된 ICMP Redirect 메시지를 이용하여 호스트가 잘못된 경로를 선택하도록 유도하는 공격이다. 제시문의 공격은 올바르게는 Smurf 공격이다.

오답 포인트

ICMP를 이용한다는 공통점만 보고 ④를 고르면 안 된다. 제시문의 결정적 단서는 Echo 패킷, 브로드캐스트 주소, 피해자로 위조한 출발지 주소, 다수의 Reply 집중이라는 조합이다.

다시 나오면 이렇게 판단

위조된 피해자 주소의 ping을 브로드캐스트로 보내 여러 장비의 응답이 피해자에게 몰리는 구조이면 Smurf 공격으로 판단한다. 비정상 IP 단편이면 Teardrop, 대량 UDP 패킷이면 UDP flooding, 경로 변경을 유도하는 Redirect 메시지이면 ICMP redirection으로 구분한다.

암기 포인트

Smurf는 '피해자 주소 위조 + 브로드캐스트 ping + Echo Reply 증폭'이다.

NoteBase

문 2. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 적절한 프로그램은 무엇인가?

① ps
② Nmap
③ nslookup
④ traceroute

정답 2번

출제 포인트

열려 있는 포트를 탐지하는 도구와 프로세스 확인·DNS 조회·경로 추적 도구를 구별하는 문제이다.

핵심 개념

Nmap은 호스트 탐지와 포트 스캔 등을 수행하는 네트워크 조사 도구이다. 대상 서버의 포트를 스캔하면 백도어와 연관된 포트가 열려 있는지 확인할 수 있다.
ps는 실행 중인 프로세스를 확인하고, nslookup은 DNS 정보를 조회하며, traceroute는 목적지까지의 네트워크 경로를 추적한다.

선지별 해설

① X — ps는 리눅스에서 실행 중인 프로세스의 상태와 목록을 확인하는 명령이다. 열린 네트워크 포트를 스캔하는 도구라는 표현이 틀리며, 올바르게는 프로세스 확인 도구이다.
② O — Nmap은 대상 호스트의 포트를 스캔하여 포트의 개방 여부를 조사할 수 있으므로 백도어 관련 포트 확인에 적절하다.
③ X — nslookup은 도메인 이름과 IP 주소 등 DNS 정보를 조회하는 명령이다. 열린 포트를 확인하는 도구라는 표현이 틀리며, 올바르게는 DNS 질의 도구이다.
④ X — traceroute는 패킷이 목적지까지 거치는 라우터와 홉 경로를 확인하는 명령이다. 열린 포트를 스캔하는 도구라는 표현이 틀리며, 올바르게는 네트워크 경로 추적 도구이다.

오답 포인트

ps도 침입 흔적 조사에 활용될 수 있지만 확인 대상은 프로세스이다. 이 문항의 핵심 표현인 '포트가 열려 있는지'는 포트 스캔 기능을 가진 Nmap을 가리킨다.

다시 나오면 이렇게 판단

문제에서 요구하는 확인 대상을 먼저 구분한다. 포트 개방 여부는 Nmap, 실행 프로세스는 ps, DNS 정보는 nslookup, 통신 경로는 traceroute로 판단한다.

NoteBase

암기 포인트

Nmap은 포트, ps는 프로세스, nslookup은 DNS, traceroute는 경로이다.

NoteBase

문 3. VPN(Virtual Private Network)에 대한 설명으로 가장 옳지 않은 것은?

① 공중망을 사용하여 사설망과 같은 효과를 얻는다.

② 서로 다른 통신 프로토콜을 사용하여 네트워크 사이에서 데이터를 전송한다.

③ RSVP 프로토콜을 사용하여 터널을 만들고 암호화를 수행한다.

④ 터널링 기법은 IPsec, SSL 등의 방법을 사용한다.

정답 3번

출제 포인트

VPN의 기본 원리인 공중망 활용, 터널링, 암호화와 RSVP의 기능을 구별하는 문제이다.

핵심 개념

VPN은 인터넷 같은 공중망 위에 논리적으로 분리된 사설 통신 경로를 구성하여 원격 사용자나 떨어진 사설망을 안전하게 연결하는 기술이다. 터널링은 원래 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 전송하는 방식이며, IPsec이나 SSL/TLS 계열 기술로 인증·무결성 보호·암호화 등을 제공할 수 있다. RSVP는 통신 경로의 자원을 예약하여 서비스 품질(QoS)을 지원하는 프로토콜이지, VPN 터널 생성과 암호화를 담당하는 프로토콜이 아니다.

선지별 해설

① O — VPN은 인터넷 같은 공중망을 이용하면서도 논리적으로 분리된 사설망과 같은 통신 환경을 제공한다.
② O — 터널링은 한 프로토콜의 패킷을 다른 프로토콜 형식 안에 캡슐화하므로, 서로 다른 네트워크 구간을 거쳐 원래 데이터를 전달할 수 있다.
③ X — 틀린 표현은 ‘RSVP 프로토콜을 사용하여 터널을 만들고 암호화를 수행한다’이다. RSVP는 네트워크 자원을 예약하여 QoS를 지원한다. 올바르게는 IPsec이나 SSL/TLS 기반 방식 등이 VPN의 보호된 터널 구성과 암호화에 사용된다고 해야 한다.
④ O — IPsec VPN과 SSL/TLS VPN은 대표적인 VPN 구현 방식이며, 터널링과 보안 기능을 제공한다.

오답 포인트

③은 네트워크 프로토콜이라는 공통점만으로 RSVP를 VPN 보안 프로토콜처럼 바꿔 놓았다. RSVP의 핵심어는 자원 예약과 QoS이고, VPN의 핵심어는 터널링과 암호화이다.

다시 나오면 이렇게 판단

프로토콜의 목적을 먼저 구분한다. 자원 예약·QoS가 목적이면 RSVP이고, 사설 통신 경로 구성·캡슐화·암호화가 목적이면 VPN 관련 기술이다.

NoteBase

암기 포인트

VPN은 터널링·암호화, RSVP는 자원 예약·QoS이다.

NoteBase

문 4. 컴퓨터의 내부 자료를 탈취하는 수법으로 프로그램 개발 시에 내용을 볼 수 있는 부정루틴을 삽입하여 컴퓨터의 정비나 유지보수를 핑계 삼아 악의적인 행위를 하는 방법은 무엇인가?

① Trap Door

② TRINOO

③ Trojan Horse

④ Teardrop

정답 1번

출제 포인트

프로그램에 비밀 접근 경로를 미리 심는 Trap Door와 분산 서비스 거부 공격 도구, 악성 프로그램, 서비스 거부 공격 기법을 구별하는 문제이다.

핵심 개념

Trap Door는 프로그램 개발 단계에서 정상적인 인증이나 통제 절차를 우회할 수 있는 비밀 진입 수단을 삽입해 두고, 정비나 유지보수 등을 명분으로 시스템에 부정 접근하는 수법이다. Back Door와 같은 뜻으로 쓰인다. TRINOO는 여러 감염 시스템을 동원하는 분산 서비스 거부 공격 도구이고, Trojan Horse는 정상 프로그램으로 위장한 악성 프로그램이며, Teardrop은 비정상적으로 겹치는 IP 단편을 보내 재조립 과정의 오류를 일으키는 서비스 거부 공격이다.

선지별 해설

① O — Trap Door는 개발자가 프로그램 내부에 숨겨 둔 부정 루틴이나 비밀 통로를 이용해 정상적인 보안 절차를 우회하는 수법이므로 제시된 설명과 일치한다.
② X — TRINOO는 프로그램에 유지보수용 비밀 통로를 삽입하는 수법이 아니다. 틀린 표현은 'TRINOO'이며, 올바르게는 'Trap Door'이다. TRINOO는 다수의 시스템을 이용해 목표에 트래픽을 집중시키는 분산 서비스 거부 공격 도구이다.
③ X — Trojan Horse는 유지보수용 부정 루틴 자체를 뜻하지 않는다. 틀린 표현은 'Trojan Horse'이며, 올바르게는 'Trap Door'이다. Trojan Horse는 유용하거나 정상적인 프로그램으로 위장해 사용자가 실행하도록 유도하는 악성 프로그램이다.
④ X — Teardrop은 프로그램 개발 시 비밀 접근 경로를 삽입하는 수법이 아니다. 틀린 표현은 'Teardrop'이며, 올바르게는 'Trap Door'이다. Teardrop은 서로 겹치도록 조작한 IP 단편을 보내 수신 시스템의 재조립 오류를 유발하는 서비스 거부 공격이다.

NoteBase

오답 포인트

모두 공격 관련 용어이지만 공격 지점이 다르다. ‘개발 시 삽입’, ‘부정 루틴’, ‘정비·유지보수를 구실로 한 비밀 접근’은 Trap Door의 결정적 단서이다.

다시 나오면 이렇게 판단

비밀 통로를 코드에 미리 심어 정상 인증을 우회하면 Trap Door, 정상 프로그램으로 위장하면 Trojan Horse, 다수의 감염 시스템으로 트래픽을 집중시키면 TRINOO, 겹치는 IP 단편으로 재조립 오류를 일으키면 Teardrop으로 판단한다.

암기 포인트

Trap Door는 숨겨 둔 문, Trojan Horse는 위장, TRINOO는 분산 공격, Teardrop은 IP 단편 공격이다.

NoteBase

문 5. 다음의 설명에 해당되는 시스템은 무엇인가?

기업 데이터 유출 방지를 의미하며 사용자가 사무실, 현장 및 집 어느 곳에서 업무 중이라도 사용자의 PC에서 기업 내 기밀 데이터가 외부로 반출되는 것을 항시 감시하고 기록하며, 정책에 따라 유출을 차단시키는 것을 주 기능으로 구현한 솔루션이다.

① DLP

② IDS

③ IDC

④ EIP

정답 1번

출제 포인트

기업의 기밀 데이터가 단말기에서 외부로 유출되는 행위를 감시·기록하고 정책에 따라 차단하는 보안 솔루션을 구별하는 문제이다.

핵심 개념

DLP(Data Loss Prevention)는 중요 정보의 외부 유출을 탐지하고 통제하는 데이터 유출 방지 솔루션이다. IDS는 침입 탐지, IDC는 전산 설비 운영 공간, EIP는 기업 정보의 통합 제공에 초점이 있다.

선지별 해설

① O — DLP는 PC 등 단말기에서 기밀 데이터의 이동을 지속적으로 감시·기록하고, 보안 정책에 위배되는 외부 반출을 차단하므로 제시된 설명과 일치한다.
② X — 설명에 해당하는 시스템을 IDS로 본 부분이 틀리다. IDS(Intrusion Detection System)는 네트워크나 시스템에 대한 침입 및 이상 행위를 탐지하는 시스템이며, 제시된 설명에 해당하는 것은 DLP이다.
③ X — 설명에 해당하는 시스템을 IDC로 본 부분이 틀리다. IDC(Internet Data Center)는 서버와 네트워크 장비를 안정적으로 운영하도록 시설·회선·전원 등을 제공하는 데이터센터이며, 제시된 설명에 해당하는 것은 DLP이다.
④ X — 설명에 해당하는 시스템을 EIP로 본 부분이 틀리다. EIP(Enterprise Information Portal)는 기업 안팎의 정보를 통합하여 사용자에게 제공하는 기업 정보 포털이며, 제시된 설명에 해당하는 것은 DLP이다.

오답 포인트

‘항시 감시’라는 표현만 보고 침입을 감시하는 IDS를 고르기 쉽다. 그러나 이 문항의 감시 대상은 침입 행위가 아니라 기밀 데이터의 외부 반출이며, 정책 위반 시 유출을 차단한다는 점이 DLP의 결정적 단서이다.

NoteBase

다시 나오면 이렇게 판단

기밀 정보·외부 반출·유출 차단이 핵심이면 DLP, 공격·침입·이상 행위 탐지가 핵심이면 IDS로 구별한다.

암기 포인트

DLP는 데이터 유출 방지, IDS는 침입 탐지이다.

NoteBase

문 6. 다음에서 설명하는 것을 올바르게 짝지은 것은?

(가)은/는 악의적인 프로그램을 건전한 프로그램처럼 포장하여 일반 사용자들이 의심 없이 자신의 컴퓨터 안에서 이를 실행시키고 실행된 (가)은/는 특정 포트를 열어 공격자의 침입을 돕고 추가적으로 정보를 자동 유출하며 자신의 존재를 숨긴다.
(나)은/는 OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격 코드 및 프로그램을 의미한다.

① (가): Exploit, (나): Trojan
② (가): Trojan, (나): Hoax
③ (가): Trojan, (나): Exploit
④ (가): Exploit, (나): Hoax

정답 3번

출제 포인트

악성 프로그램의 위장·실행 방식인 트로이 목마(Trojan)와 취약점을 이용하는 공격 수단인 익스플로잇(Exploit)을 구별하는 문제이다.

핵심 개념

Trojan: 정상적이거나 유용한 프로그램처럼 위장하여 사용자가 직접 실행하게 만드는 악성 프로그램이다. 실행 뒤 백도어를 열거나 정보를 유출하고 자신의 존재를 숨길 수 있다.
Exploit: 운영체제나 응용 프로그램의 취약점을 이용하여 권한을 획득하거나 특정 동작을 수행하는 공격 코드 또는 프로그램이다.
Hoax: 실제 악성코드 자체가 아니라 거짓 경고나 허위 정보를 퍼뜨려 사용자의 불필요하거나 잘못된 행동을 유도하는 기만이다.
핵심 구분은 '정상 프로그램으로 위장'하면 Trojan, '버그·취약점 이용'이면 Exploit이라는 점이다.

NoteBase

선지별 해설

① X — (가)를 Exploit, (나)를 Trojan으로 서로 바꾸어 짝지었다. 올바르게는 (가)가 Trojan이고 (나)가 Exploit이다.
② X — (가)의 Trojan은 맞지만 (나)의 Hoax가 틀렸다. OS의 버그를 이용해 루트 권한을 얻거나 특정 기능을 수행하는 공격 코드는 Exploit이다.
③ O — 정상 프로그램처럼 위장하여 사용자가 실행하게 하고 백도어 개설·정보 유출 등을 수행하는 (가)는 Trojan이며, OS의 버그를 이용하는 공격 코드인 (나)는 Exploit이다.
④ X — 두 용어가 모두 틀렸다. (가)는 Exploit이 아니라 Trojan이고, (나)는 Hoax가 아니라 Exploit이다. Hoax는 취약점 공격 코드가 아니라 거짓 경고나 허위 정보로 사용자를 속이는 행위이다.

오답 포인트

Trojan도 침입을 돕고 정보를 유출하므로 공격 기능만 보면 Exploit과 혼동하기 쉽다. 그러나 이 문항의 결정적 단서는 (가)의 '건전한 프로그램처럼 포장하여 사용자가 실행'과 (나)의 'OS의 버그를 이용'이다.

다시 나오면 이렇게 판단

설명의 동작 결과보다 최초 침투·작동 방식을 확인한다. 정상 프로그램으로 위장해 실행을 유도하면 Trojan, 소프트웨어의 버그나 취약점을 직접 이용하면 Exploit, 거짓 경고로 사용자를 속이면 Hoax로 판단한다.

암기 포인트

Trojan은 위장 실행, Exploit은 취약점 이용, Hoax는 거짓 경고이다.

NoteBase

문 7. 다음에서 설명하는 것은 무엇인가?

무선네트워크 액세스포인트 이름을 의미하며 각 액세스포인트에 하나씩 할당되어 있다. 기본적으로 AP와 Client는 이것이 일치해야만 통신이 가능하게 되는데 액세스포인트가 자신들의 이것을 브로드캐스팅하기 때문에 보안에 취약할 수밖에 없다.

① SSID

② MAC

③ WEP

④ WPA

정답 1번

출제 포인트

무선 네트워크의 이름을 나타내고 AP와 클라이언트가 같은 네트워크를 식별하는 데 사용하는 값이 SSID임을 묻는 문제이다.

핵심 개념

SSID(Service Set Identifier)는 무선 LAN을 식별하는 네트워크 이름이다. AP는 일반적으로 비콘 프레임을 통해 SSID를 알리며, 클라이언트는 접속하려는 무선 네트워크의 SSID를 선택하여 연결한다.
MAC 주소는 네트워크 인터페이스의 식별 주소이고, WEP와 WPA는 무선 통신을 보호하기 위한 보안 방식이다.

선지별 해설

① O — SSID는 무선 네트워크를 식별하는 이름이다. AP가 이를 브로드캐스트할 수 있고 클라이언트가 같은 SSID를 기준으로 접속한다는 지문의 설명과 일치한다.
② X — 틀린 표현은 ‘MAC’이다. MAC 주소는 네트워크 인터페이스를 식별하는 주소이며, 무선 네트워크의 이름은 SSID이다.
③ X — 틀린 표현은 ‘WEP’이다. WEP는 무선 통신의 기밀성을 보호하기 위한 암호화·인증 방식이며, AP의 네트워크 이름은 SSID이다.
④ X — 틀린 표현은 ‘WPA’이다. WPA는 WEP의 보안 취약점을 보완하기 위해 도입된 무선 보안 방식이며, AP의 네트워크 이름은 SSID이다.

오답 포인트

지문에 ‘보안에 취약’이라는 표현이 있어 WEP나 WPA를 고르기 쉽다. 그러나 정답을 결정하는 핵심 단서는 ‘액세스포인트 이름’, ‘AP와 Client가 일치’, ‘브로드캐스팅’이며 이는 SSID의 특성이다.

NoteBase

다시 나오면 이렇게 판단

무선 네트워크의 이름이나 접속 대상을 구별하는 값이면 SSID, 장치의 네트워크 인터페이스 주소이면 MAC 주소, 무선 구간의 암호화·인증 방식이면 WEP 또는 WPA로 판단한다.

암기 포인트

SSID는 무선망의 이름, MAC은 인터페이스의 주소, WEP·WPA는 무선 보안 방식이다.

NoteBase

문 8. 이더넷 물리 주소가 될 수 있는 것은 다음 중 어떤 것인가?

① 01:02:01:2C:4B

② 07:01:02:01:2C:4B:2C

③ 07:01:02:01:2C:4B

④ 07:02:01:02:3B:4C:3C:2B

정답 3번

출제 포인트

이더넷 물리 주소인 MAC 주소의 길이와 표기 형식을 판별하는 문제이다.

핵심 개념

이더넷 MAC 주소는 48비트, 즉 6옥텟으로 구성된다. 일반적으로 각 옥텟을 두 자리 16진수로 나타내고 콜론(:)으로 구분하므로, 전체가 6개의 16진수 묶음이어야 한다. 각 묶음의 값은 00부터 FF까지이다.

선지별 해설

① X — 01:02:01:2C:4B는 두 자리 16진수 묶음이 5개뿐이므로 40비트 주소이다. 틀린 부분은 5개 옥텟이라는 점이며, 이더넷 MAC 주소는 6개 옥텟이어야 한다.
② X — 07:01:02:01:2C:4B:2C는 묶음이 7개이므로 56비트 주소이다. 틀린 부분은 7개 옥텟이라는 점이며, 6개 옥텟으로 표기해야 한다.
③ O — 07:01:02:01:2C:4B는 두 자리 16진수 묶음이 정확히 6개이고 각 묶음도 00부터 FF의 범위에 있으므로 이더넷 물리 주소가 될 수 있다.
④ X — 07:02:01:02:3B:4C:3C:2B는 묶음이 8개이므로 64비트 주소이다. 틀린 부분은 8개 옥텟이라는 점이며, 이더넷 MAC 주소는 6개 옥텟이어야 한다.

오답 포인트

각 묶음이 모두 정상적인 16진수처럼 보이므로 묶음의 개수를 놓치기 쉽다. 이 문제의 핵심은 값의 모양보다 콜론으로 구분된 두 자리 묶음이 정확히 6개인지 확인하는 데 있다.

다시 나오면 이렇게 판단

콜론으로 나뉜 묶음의 수를 먼저 센다. 두 자리 16진수 묶음이 6개이면 48비트 이더넷 MAC 주소 형식에 맞고, 그다음 각 묶음이 00부터 FF의 범위인지 확인한다.

암기 포인트

MAC 주소는 48비트 = 6옥텟 = 두 자리 16진수 6묶음이다.

NoteBase

문 9. 아래의 하드웨어 장비 중 OSI 2계층에 해당하는 장비는 무엇인가?

리피터, 허브, 브리지, 라우터, 스위치, L4 스위치

① 리피터, 허브
② 브리지, 스위치
③ 라우터, 스위치
④ 스위치, L4 스위치

정답 2번

출제 포인트

OSI 계층별 네트워크 장비를 구분하는 문제이다. 장비가 주소와 정보를 어느 계층 수준에서 처리하는지가 판단 기준이다.

핵심 개념

1계층 장비인 리피터와 허브는 전기·물리 신호를 전달하거나 증폭한다. 2계층 장비인 브리지와 스위치는 프레임의 MAC 주소를 보고 전달한다. 3계층 장비인 라우터는 패킷의 IP 주소를 보고 경로를 선택한다. L4 스위치는 전송 계층의 포트 번호 등으로 트래픽을 분배한다.

선지별 해설

① X — 리피터와 허브는 모두 OSI 1계층 장비이다. 틀린 부분은 두 장비를 2계층 장비로 본 점이며, 올바르게는 '1계층 장비는 리피터와 허브이다'가 된다.
② O — 브리지와 스위치는 프레임의 MAC 주소를 이용해 전달 여부와 포트를 결정하므로 모두 OSI 2계층 장비이다.
③ X — 라우터는 3계층, 스위치는 2계층 장비이므로 둘 다 2계층에 해당하지 않는다. 틀린 부분은 '라우터'이며, 이를 '브리지'로 고치면 2계층 장비의 조합이 된다.
④ X — 일반적인 스위치는 2계층이지만 L4 스위치는 4계층 정보를 이용하므로 둘 다 2계층에 해당하지 않는다. 틀린 부분은 'L4 스위치'이며, 이를 '브리지'로 고치면 2계층 장비의 조합이 된다.

오답 포인트

'스위치'라는 공통 명칭 때문에 일반 스위치와 L4 스위치를 같은 계층으로 보기 쉽다. 일반적인 스위치는 MAC 주소를 처리하는 2계층 장비이지만, L4 스위치는 포트 번호 등 전송 계층 정보를 처리한다.

NoteBase

다시 나오면 이렇게 판단

신호는 1계층, MAC 주소와 프레임은 2계층, IP 주소와 패킷은 3계층, 포트 번호는 4계층으로 연결해 장비를 분류한다.

암기 포인트

리피터·허브는 1계층, 브리지·스위치는 2계층, 라우터는 3계층, L4 스위치는 4계층이다.

NoteBase

문 10. 다음 지문의 필터링 규칙을 설명한 것 중에서 가장 옳지 않은 것은?

가. iptables -A INPUT -s 201.1.1.1 -j DROP
나. iptables -A INPUT -p TCP -j ACCEPT
다. iptables -A INPUT -i eth0 -p TCP -dport 80 -j DROP
라. iptables -A INPUT -i eth0 -p TCP -dport 80 -j REJECT

① “가”번은 201.1.1.1에서 유입되는 모든 패킷을 DROP 시킨다.

② “나”번은 TCP 프로토콜을 사용하는 모든 서비스의 요청을 허용한다.

③ “다”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP 시킨다.

④ “라”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP하고 송신자는 차단 여부를 확인할 수 없게 한다.

정답 4번

출제 포인트

iptables의 INPUT 체인 규칙에서 출발지 주소, 입력 인터페이스, 프로토콜, 목적지 포트 조건을 읽고 DROP과 REJECT의 처리 방식 차이를 구별하는 문제이다.

핵심 개념

INPUT 체인은 로컬 시스템으로 들어오는 패킷을 검사한다. -s는 출발지 주소, -i는 패킷이 들어온 인터페이스, -p는 프로토콜, dport는 목적지 포트를 조건으로 지정한다. ACCEPT는 조건에 맞는 패킷을 허용하고, DROP은 응답 없이 폐기하며, REJECT는 패킷을 거부하면서 송신자에게 거부 응답을 보낸다.

선지별 해설

① O — ‘가’는 출발지 주소가 201.1.1.1인 패킷이 INPUT 체인으로 들어오면 DROP하도록 지정한다. 별도의 프로토콜이나 포트 조건이 없으므로 해당 출발지의 모든 프로토콜 패킷이 대상이다.
② O — ‘나’는 INPUT 체인에 들어오는 TCP 패킷을 ACCEPT한다. 포트 조건이 없으므로 TCP를 사용하는 특정 서비스에 한정하지 않고 모든 목적지 포트의 TCP 요청을 허용한다.
③ O — ‘다’는 eth0으로 들어오고 TCP를 사용하며 목적지 포트가 80번인 패킷을 DROP한다. 따라서 조건에 맞는 웹 서비스 요청 패킷은 응답 없이 폐기된다.
④ X — 틀린 부분은 REJECT를 ‘DROP하고 송신자가 차단 여부를 확인할 수 없게 한다’고 설명한 것이다. 올바르게는 ‘라’가 조건에 맞는 패킷을 REJECT하고 송신자에게 거부 응답을 보내므로 송신자가 차단 또는 접속 거부 사실을 알 수 있게 한다.

NoteBase

오답 포인트

④의 REJECT를 DROP과 같은 무응답 폐기로 본 것이 함정이다. 두 동작 모두 통신을 막지만, DROP은 침묵하고 REJECT는 거부 사실을 응답으로 알린다.

다시 나오면 이렇게 판단

먼저 INPUT 뒤의 조건을 출발지(-s), 인터페이스(-i), 프로토콜(-p), 목적지 포트(dport) 순서로 묶은 뒤 마지막 동작을 확인한다. 마지막이 DROP이면 무응답 폐기, REJECT이면 거부 응답 전송으로 판단한다.

암기 포인트

DROP은 조용히 버리고, REJECT는 거부했다고 알린다.

NoteBase

문 11. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기

② 패킷을 송신하고 수신하는 프로세스의 포트 번호

③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호

④ 송신 시스템의 TCP 패킷의 생성 시간

정답 4번

출제 포인트

TCP 헤더에 실제로 존재하는 필드와 헤더만으로 알 수 없는 정보를 구분하는 문제이다.

핵심 개념

TCP 헤더는 출발지·목적지 포트 번호, 순서 번호, 확인응답 번호, 윈도우 크기 등 TCP 통신 제어에 필요한 정보를 담는다. 반면 기본 TCP 헤더에는 패킷의 생성 시각을 기록하는 필드가 없다.

선지별 해설

① X — '수신 시스템이 처리할 수 있는 윈도우 크기'는 검출할 수 없는 정보가 아니다. TCP 헤더의 Window Size 필드에는 수신측이 광고하는 수신 윈도우 크기가 들어 있으므로, 올바르게는 TCP 헤더에서 확인할 수 있는 정보이다.
② X — '패킷을 송신하고 수신하는 프로세스의 포트 번호'는 검출할 수 없는 정보가 아니다. TCP 헤더에는 Source Port와 Destination Port 필드가 있으므로, 올바르게는 송신측과 수신측의 포트 번호를 확인할 수 있다.
③ X — '수신측에서 앞으로 받고자 하는 바이트의 순서 번호'는 검출할 수 없는 정보가 아니다. ACK 플래그가 설정된 TCP 세그먼트의 Acknowledgment Number는 수신측이 다음에 받기를 기대하는 바이트의 순서 번호이므로, 올바르게는 TCP 헤더에서 확인할 수 있다.
④ O — 기본 TCP 헤더에는 'TCP 패킷의 생성 시간'을 나타내는 필드가 없으므로 이를 검출할 수 없다. TCP Timestamp 옵션이 사용되더라도 그 값은 송신 시스템의 절대적인 패킷 생성 시간을 직접 나타내는 필드가 아니다.

오답 포인트

③의 확인응답 번호를 이미 받은 마지막 바이트 번호로 착각하거나, 선택적으로 붙는 TCP Timestamp 옵션을 곧바로 패킷 생성 시간으로 해석하기 쉽다. 확인응답 번호는 다음에 기대하는 바이트 번호이며, 기본 TCP 헤더에는 생성 시각 필드가 없다.

NoteBase

다시 나오면 이렇게 판단

TCP 기본 헤더의 대표 필드인 포트 번호, 순서 번호, 확인응답 번호, 윈도우 크기와 대조한다. 시간 정보가 제시되면 기본 헤더 필드인지, 선택적 옵션인지, 실제 생성 시각을 뜻하는지를 구분한다.

암기 포인트

TCP 기본 헤더에는 포트·순서·확인응답·윈도우는 있지만 패킷 생성 시간은 없다.

NoteBase

문 12. 다음 중 IPsec(IP Security Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① IPsec 정책 설정 과정에서 송·수신자의 IP주소를 입력한다.

② 전송(Transport) 모드에서는 IP헤더가 암호화된다.

③ 재전송 공격을 막기 위해 IP 패킷별로 순서번호를 부여한다.

④ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.

정답 2번

출제 포인트

IPsec의 정책 설정, 전송 모드의 보호 범위, 재전송 공격 방지 방식, IKE의 역할을 구분하는 문제이다.

핵심 개념

IPsec은 IP 계층에서 통신의 기밀성·무결성·인증 등을 제공하는 보안 기술이다. 전송 모드는 원래 IP 헤더를 남겨 두고 주로 상위 계층의 데이터 부분을 보호하며, 터널 모드는 원래 IP 패킷 전체를 캡슐화하고 새로운 외부 IP 헤더를 붙인다.

선지별 해설

① O — IPsec 정책은 어떤 트래픽에 보안을 적용할지를 식별해야 하므로 송신자와 수신자의 IP 주소를 트래픽 선택 조건으로 설정할 수 있다.
② X — 틀린 표현은 '전송(Transport) 모드에서는 IP헤더가 암호화된다'이다. 전송 모드에서는 원래 IP 헤더가 암호화되지 않고 주로 IP 페이로드가 보호된다. 원래 IP 패킷 전체를 보호하고 새 외부 IP 헤더를 덧붙이는 방식은 터널 모드이다.
③ O — IPsec의 AH 또는 ESP는 보안 연관마다 패킷에 증가하는 순서번호를 넣고 수신 측이 재전송 방지 창으로 중복 패킷을 판별하여 재전송 공격을 막는다.
④ O — IKE는 통신 당사자를 인증하고 보안 연관을 협상하면서 IPsec 통신에 사용할 키를 안전하게 생성·교환하는 프로토콜이다.

오답 포인트

②는 전송 모드와 터널 모드의 보호 범위를 바꾸어 놓았다. '전송'이라는 말 때문에 패킷 전체가 암호화된다고 생각하기 쉽지만, 전송 모드에서는 라우팅에 필요한 원래 IP 헤더가 노출된다.

다시 나오면 이렇게 판단

원래 IP 헤더의 처리 여부를 먼저 본다. 원래 IP 헤더를 유지하고 페이로드를 보호하면 전송 모드이고, 원래 IP 패킷 전체를 캡슐화한 뒤 새 IP 헤더를 붙이면 터널 모드이다. 순서번호는 재전송 방지, IKE는 인증·보안 연관 협상·키 교환과 연결한다.

NoteBase

암기 포인트

전송 모드: 원래 IP 헤더는 그대로, 페이로드 보호. 터널 모드: 원래 IP 패킷 전체를 감싸고 새 IP 헤더 추가.

NoteBase

문 13. 다음 설명에 해당하는 블루투스 공격 방법은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여, 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf)
② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug)
④ 블루재킹(BlueJacking)

정답 1번

출제 포인트

블루투스 공격을 공격 행위와 피해 유형으로 구별하는 문제이다. 인증 없이 OPP를 악용하여 주소록·일정 또는 파일을 빼내는 행위는 블루스나프에 해당한다.

핵심 개념

블루스나프(BlueSnarf): 취약한 블루투스 장치에 무단으로 접속하여 주소록, 일정, 파일 등 저장 정보를 탈취하는 공격이다. 키워드는 '정보·파일 무단 열람 및 탈취'이다.
블루프린팅(BluePrinting): 블루투스 장치가 제공하는 정보를 수집하여 제조사, 모델, 펌웨어 버전 등을 식별하는 장치 지문 수집 기법이다. 키워드는 '장치 식별'이다.
블루버그(BlueBug): 취약점을 이용해 대상 장치의 명령 기능을 장악하여 통화 발신, 메시지 전송, 도청 등을 수행하는 공격이다. 키워드는 '장치 제어'이다.
블루재킹(BlueJacking): 블루투스를 통해 상대 장치에 원치 않는 메시지나 전자 명함 등을 보내는 행위이다. 키워드는 '비요청 메시지 전송'이다.

NoteBase

선지별 해설

① O — 블루스나프는 인증되지 않은 접근으로 대상 장치의 주소록·일정·파일과 같은 정보를 열람하거나 탈취하는 공격이다. 제시문의 OPP 악용과 임의 파일 접근이 이에 해당한다.
② X — 블루프린팅을 파일 탈취 공격으로 본 부분이 틀리다. 올바르게는 블루프린팅은 장치가 노출하는 정보를 이용해 제조사, 모델, 펌웨어 버전 등을 식별하는 기법이다.
③ X — 블루버그를 OPP를 이용한 정보·파일 열람 공격으로 본 부분이 틀리다. 올바르게는 블루버그는 대상 장치의 명령 기능을 장악하여 통화 발신, 메시지 전송, 도청 등 장치 기능을 몰래 제어하는 공격이다.
④ X — 블루재킹을 정보·파일 탈취 공격으로 본 부분이 틀리다. 올바르게는 블루재킹은 블루투스를 이용해 상대에게 원치 않는 메시지나 전자 명함 등을 보내는 행위이다.

오답 포인트

네 공격 모두 이름이 ‘Blue’로 시작하지만 목적이 다르다. 제시문의 ‘주소록 또는 달력 열람’과 ‘파일 접근’은 단순한 장치 식별이나 메시지 전송이 아니라 저장 정보의 무단 탈취이므로 블루스나프를 고르는 단서이다.

다시 나오면 이렇게 판단

공격 결과를 먼저 확인한다. 저장 정보·파일 탈취는 블루스나프, 제조사·모델 식별은 블루프린팅, 통화·메시지 등 장치 기능 제어는 블루버그, 원치 않는 메시지 전송은 블루재킹으로 판단한다.

암기 포인트

스나프는 정보 탈취, 프린팅은 장치 식별, 버그는 장치 제어, 재킹은 메시지 전송이다.

NoteBase

문 14. 다음의 보기에서 설명하고 있는 접근제어(Access Control) 방법은 무엇인가?

· 주체(사용자)의 객체(정보)에 대한 접근이 주체의 비밀취급인가 레이블과 각 객체에 부여된 민감도 레이블에 따라 접근 허용 여부를 결정하는 방식
· 중앙집중적 관리가 가능하고, 기밀성이 매우 중요한 조직에서 사용
· 다단계 보안 모델이라고 부르기도 함

① 임의적 접근제어
② 강제적 접근제어
③ 역할기반 접근제어
④ 자율적 접근제어

정답 2번

출제 포인트

주체의 비밀취급인가 레이블과 객체의 민감도 레이블을 비교하여 접근을 통제하는 강제적 접근제어(MAC)의 특징을 묻는 문제이다.

핵심 개념

강제적 접근제어(MAC)는 중앙 관리자가 정한 보안 정책과 보안 레이블에 따라 접근 권한을 강제하는 방식이다.
주체의 비밀취급인가 수준과 객체의 민감도 등급을 비교하므로 다단계 보안에 적합하다.
임의적·자율적 접근제어(DAC)는 객체의 소유자가 사용자나 그룹을 기준으로 접근 권한을 부여하거나 회수하는 방식이다.
역할기반 접근제어(RBAC)는 직무나 역할에 권한을 묶고 사용자에게 역할을 부여하는 방식이다.

선지별 해설

① X — 임의적 접근제어는 객체 소유자가 신원이나 그룹을 기준으로 접근 권한을 정하는 방식이다. 틀린 표현은 '임의적 접근제어'이며, 보기의 설명에 맞게 고치면 '강제적 접근제어'이다.
② O — 강제적 접근제어는 주체와 객체의 보안 레이블을 대조하여 중앙의 보안 정책에 따라 접근 허용 여부를 결정한다. 기밀성이 중요한 조직의 다단계 보안 모델이라는 설명과도 일치한다.
③ X — 역할기반 접근제어는 사용자 개인이나 보안 레이블이 아니라 직무·역할에 권한을 연결한다. 틀린 표현은 '역할기반 접근제어'이며, 보기의 설명에 맞게 고치면 '강제적 접근제어'이다.
④ X — 자율적 접근제어는 일반적으로 객체 소유자가 권한을 자율적으로 정하는 임의적 접근제어 계열을 뜻한다. 틀린 표현은 '자율적 접근제어'이며, 보기의 설명에 맞게 고치면 '강제적 접근제어'이다.

NoteBase

오답 포인트

‘강제적’이라는 말만 보고 사용자의 행동을 강제로 제한한다는 막연한 뜻으로 판단하면 안 된다. 이 문항의 결정적 단서는 비밀취급인가 레이블, 민감도 레이블, 중앙집중적 관리, 다단계 보안이다. 또한 임의적 접근제어와 자율적 접근제어는 표현이 달라도 객체 소유자의 재량을 중심으로 한다는 점이 같다.

다시 나오면 이렇게 판단

보안등급·민감도·레이블·다단계 보안이 나오면 MAC, 객체 소유자의 재량이 나오면 DAC, 직무·역할에 따른 권한 부여가 나오면 RBAC로 판단한다.

암기 포인트

MAC는 레이블, DAC는 소유자, RBAC는 역할이다.

NoteBase

문 15. 침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는데 적합한 기법은 무엇인가?

① 규칙 기반의 오용 탐지

② 통계적 분석에 의한 이상 탐지

③ 전문가 시스템을 이용한 오용 탐지

④ 시그니처 기반(Signature based) 탐지

정답 2번

출제 포인트

이 문제는 알려진 공격 패턴을 찾는 오용 탐지와 정상 상태에서 벗어난 행동을 찾는 이상 탐지의 차이를 묻는다.

핵심 개념

오용 탐지는 미리 정의된 공격 규칙이나 시그니처와 일치하는 행위를 찾는 방식으로, 알려진 공격 탐지에 강하다. 이상 탐지는 정상적인 사용 행태를 통계적으로 학습한 뒤 정상 범위를 벗어난 변화를 찾으므로 알려지지 않은 공격도 탐지할 수 있다.

선지별 해설

① X

규칙 기반의 오용 탐지는 미리 정의된 공격 규칙과 일치하는지를 검사하므로 알려진 공격 탐지에 적합하다. 틀린 표현은 '오용 탐지'이며, 알려지지 않은 공격에는 정상 행태와의 차이를 찾는 이상 탐지가 더 적합하다.

② O

통계적 분석에 의한 이상 탐지는 정상적인 활동의 기준을 만든 뒤 그 기준에서 크게 벗어난 행위를 탐지한다. 기존 시그니처가 없는 새로운 공격도 비정상 행태로 포착할 수 있다.

③ X

전문가 시스템을 이용한 오용 탐지는 전문가의 지식을 규칙으로 구성하여 알려진 공격 특징과 대조한다. 틀린 표현은 '오용 탐지'이며, 알려지지 않은 공격 탐지에는 통계적 분석 등에 의한 이상 탐지가 적합하다.

④ X

시그니처 기반 탐지는 공격별로 알려진 고유 패턴과의 일치 여부를 확인하므로 새로운 공격의 시그니처가 아직 없으면 탐지가 어렵다. 틀린 표현은 '시그니처 기반 탐지'이며, 알려지지 않은 공격에는 이상 탐지가 더 적합하다.

NoteBase

오답 포인트

①, ③, ④는 구현 방식이 서로 달라 보여도 모두 이미 알려진 공격의 규칙이나 패턴을 이용하는 오용 탐지 계열이다. ‘알려지지 않은 공격’이라는 표현을 놓치면 이들을 정답으로 고르기 쉽다.

다시 나오면 이렇게 판단

문제에 ‘알려진 공격·규칙·시그니처’가 나오면 오용 탐지로, ‘알려지지 않은 공격·정상 행태에서의 이탈·통계적 분석’이 나오면 이상 탐지로 판단한다.

암기 포인트

아는 공격은 오용 탐지, 모르는 공격은 이상 탐지이다.

NoteBase

문 16. VPN(Virtual Private Network)에서 “터널링”이라는 용어가 의미하는 내용에 가장 부합하는 것은?

① 선택사항으로서 작동 시 네트워크 성능을 향상시킬 수 있는 기능이다.

② 가상회선을 생성하고 유지할 목적으로 상이한 프로토콜의 패킷 안에 패킷을 캡슐화하는 기능이다.

③ 네트워크상 해커를 탐지하기 위해 시스템 관리자가 사용하는 기능이다.

④ 네트워크 침입이 탐지되면 바로 차단 조치를 취해 비정상 행위를 통제하는 기능이다.

정답 2번

출제 포인트

VPN의 터널링이 패킷 캡슐화를 통해 논리적인 가상 통신 경로를 만드는 기능임을 묻는 문제이다.

핵심 개념

터널링은 한 프로토콜의 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 공용 네트워크를 통과할 수 있는 논리적 통신 경로인 터널을 만들고 유지하는 기술이다. 터널링의 핵심 키워드는 ‘캡슐화’와 ‘가상회선’이며, 침입 탐지나 차단 기능과는 구별된다.

선지별 해설

① X — ‘네트워크 성능을 향상시키는 선택 기능’이라는 표현이 틀렸다. 터널링은 패킷을 캡슐화하여 가상 통신 경로를 구성하는 기능이며, 캡슐화 헤더 처리로 오버헤드가 생길 수도 있다.
② O — 한 프로토콜의 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 가상회선을 생성하고 유지한다는 설명은 터널링의 의미에 부합한다.
③ X — ‘해커를 탐지하는 기능’이라는 표현이 틀렸다. 네트워크의 공격이나 이상 행위를 탐지하는 기능은 침입 탐지 시스템(IDS)의 역할이고, 터널링은 패킷 캡슐화를 통한 논리적 경로 구성 기술이다.
④ X — ‘탐지 즉시 차단하여 비정상 행위를 통제하는 기능’이라는 표현이 틀렸다. 탐지와 차단을 함께 수행하는 기능은 침입 방지 시스템(IPS)의 역할이고, 터널링 자체는 침입 차단 기능이 아니다.

오답 포인트

③과 ④는 VPN을 보안 기술이라는 넓은 범주로만 기억할 때 고르기 쉽다. 그러나 터널링은 공격의 탐지·차단이 아니라 패킷을 다른 패킷 안에 넣어 전달 경로를 만드는 기술이다.

다시 나오면 이렇게 판단

터널링을 묻는 선지에서는 ‘캡슐화’, ‘상이한 프로토콜’, ‘논리적 터널 또는 가상회선’이라는 표현을 확인한다. ‘탐지’가 중심이면 IDS, ‘탐지 후 차단’이 중심이면 IPS로 구별한다.

NoteBase

암기 포인트

터널링은 캡슐화로 길을 만들고, IDS는 탐지하며, IPS는 탐지 후 차단한다.

NoteBase

문 17. 침해대응 과정에서 다음의 패킷로그를 기준으로 검토해 보았다. 어떤 공격 기법인가?

· Source IP : 203.234.212.10
· Destination IP : 203.234.212.10
· Protocol : 6
· Source Port : 21845
· Destination Port : 21845

① Land Attack
② Syn flooding Attack
③ Smurf Attack
④ Ping of Death Attack

정답 1번

출제 포인트

패킷 로그의 출발지·목적지 IP 주소와 포트 번호가 각각 같은지를 보고 LAND Attack을 식별하는 문제이다.

핵심 개념

LAND Attack은 출발지 IP 주소와 목적지 IP 주소를 공격 대상의 주소로 같게 조작하고, 출발지 포트와 목적지 포트도 같게 설정한 패킷을 보내 대상이 자기 자신에게 응답하도록 만드는 서비스 거부 공격이다.
SYN flooding Attack은 다수의 TCP 연결 요청을 보내 반개방 연결 자원을 고갈시키는 공격이고, Smurf Attack은 피해자의 IP 주소로 위조한 ICMP Echo Request를 브로드캐스트하여 증폭된 응답이 피해자에게 향하게 하는 공격이며, Ping of Death Attack은 재조립 후 허용 크기를 초과하는 비정상 IP 패킷으로 장애를 유발하는 공격이다.

NoteBase

선지별 해설

① O — 출발지 IP와 목적지 IP가 모두 203.234.212.10이고 출발지 포트와 목적지 포트도 모두 21845이다. 자기 자신을 출발지와 목적지로 삼는 이 패턴은 LAND Attack의 특징이다.
② X — 틀린 표현은 'SYN flooding Attack'이다. SYN flooding Attack은 TCP SYN을 대량으로 보내 반개방 연결 대기열을 고갈시키는 공격이다. 제시된 동일 IP·동일 포트 패턴은 실제로 LAND Attack이다.
③ X — 틀린 표현은 'Smurf Attack'이다. Smurf Attack은 피해자의 주소로 출발지 IP를 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 응답을 증폭하는 공격이다. 로그의 프로토콜 6은 TCP이고 동일 IP·동일 포트가 나타나므로 실제로 LAND Attack이다.
④ X — 틀린 표현은 'Ping of Death Attack'이다. Ping of Death Attack은 조각을 재조립했을 때 IP 패킷의 최대 허용 크기를 넘도록 만든 비정상 패킷으로 장애를 일으키는 공격이다. 제시된 로그는 크기 초과가 아니라 동일 IP·동일 포트가 핵심이므로 실제로 LAND Attack이다.

오답 포인트

프로토콜 6이 TCP라는 점만 보고 ②를 고르기 쉽다. 그러나 공격 식별의 결정적 단서는 TCP 사용 자체가 아니라 출발지와 목적지의 IP 주소 및 포트 번호가 모두 같다는 점이다.

다시 나오면 이렇게 판단

패킷 로그에서는 먼저 출발지 IP와 목적지 IP를 비교하고, 이어서 두 포트를 비교한다. IP와 포트가 모두 자기 자신을 가리키면 LAND Attack으로 판단한다.

암기 포인트

LAND는 같은 IP, 같은 포트로 자기 자신에게 착륙하는 공격이다.

NoteBase

문 18. ESM(Enterprise Security Management)에 대한 설명으로 가장 올바른 것은 무엇인가?

① 개별 솔루션 간의 별도 연동작업이 추가적으로 요구되지 않는다.

② Agent에서 읽어온 로그를 분석 없이 Manager가 수신 받고 콘솔로 표출한다.

③ 각 종 로그를 통합적으로 관리하여 통합 보안관제 서비스를 제공한다.

④ 이기종의 보안시스템을 통합하여 관리할 수 없다.

정답 3번

출제 포인트

ESM의 핵심 기능이 이기종 보안시스템에서 발생한 로그를 통합 수집·분석하여 중앙에서 보안관제를 수행하는 것임을 묻는 문제이다.

핵심 개념

ESM(Enterprise Security Management)은 방화벽, 침입탐지시스템 등 여러 보안시스템의 이벤트와 로그를 중앙에서 수집하고 상관분석하여 통합 보안관제를 지원하는 체계이다. 일반적으로 Agent가 각 보안시스템의 로그를 수집해 Manager로 전달하고, Manager는 이를 분석·관리하며, Console은 관리자가 결과를 조회하고 대응하도록 제공한다.

선지별 해설

① X — 틀린 표현은 '별도 연동작업이 추가적으로 요구되지 않는다'이다. 개별 보안 솔루션의 로그를 ESM이 수집·처리하려면 Agent나 연동 모듈의 설치·설정 등 솔루션별 연동 작업이 필요할 수 있다.
② X — 틀린 표현은 '분석 없이'이다. Manager는 Agent가 수집한 로그를 단순 수신하는 데 그치지 않고 정규화·분석·상관분석하여 보안 이벤트를 관리하며, Console은 그 결과를 관리자에게 보여 준다.
③ O — 여러 보안시스템에서 생성되는 각종 로그를 한곳에 모아 분석·관리함으로써 통합 보안관제 서비스를 제공한다는 설명은 ESM의 핵심 목적에 해당한다.
④ X — 틀린 표현은 '통합하여 관리할 수 없다'이다. ESM은 서로 다른 종류와 제조사의 보안시스템을 통합하여 중앙에서 관리·관제하기 위한 체계이다.

오답 포인트

ESM이 '통합 관리'를 제공한다는 사실을 '별도 연동작업이 전혀 필요 없다'는 뜻으로 확대하면 ①에 속기 쉽다. 또한 Manager의 역할을 단순 로그 수신으로 축소한 ②와, ESM의 목적을 정반대로 서술한 ④를 구별해야 한다.

다시 나오면 이렇게 판단

ESM 선지는 '여러 보안시스템의 로그 수집 → 중앙 분석·상관분석 → 통합 관제'의 흐름에 맞는지 확인한다. '분석 없이', '연동 불필요', '이기종 통합 불가'처럼 통합·분석 기능을 부정하는 표현은 틀린 설명으로 판단한다.

NoteBase

암기 포인트

ESM은 이기종 보안 로그의 통합 수집·분석·관제이다.

NoteBase

문 19. 특정 기관에서 사용자가 누구인가는 확인하지 않고, 그 기관이 인가한 장비이면 기관 네트워크에 접근이 가능하도록 하는 정책을 수행하고자 할 때, 적용할 수 있는 장비 인증기술로 적절한 것은?

① ID/PW 기반 인증기술

② MAC 주소 값 인증기술

③ SSID 인증기술

④ WEP 인증기술

정답 2번

출제 포인트

이 문제는 사용자의 신원을 확인하는 사용자 인증과 접속 장비 자체를 식별하는 장비 인증을 구별하는 문제이다.

핵심 개념

MAC 주소 인증은 네트워크 인터페이스에 부여된 MAC 주소를 허용 목록과 대조하여 장비의 접속 허용 여부를 판단하는 방식이다. 반면 ID/PW는 사용자를, SSID는 무선 네트워크의 이름을, WEP는 공유 키를 바탕으로 무선 구간의 접근과 통신을 보호하는 기술이다.

선지별 해설

① X — ID/PW 기반 인증기술은 입력한 계정과 비밀번호로 사용자가 누구인지 확인하는 사용자 인증이다. 틀린 부분은 이를 사용자 확인 없이 수행하는 장비 인증으로 본 점이며, 올바르게는 사용자 신원 인증기술이라고 해야 한다.
② O — MAC 주소 값을 기관이 인가한 장비의 허용 목록과 대조하면 사용자의 신원을 확인하지 않고도 해당 장비의 네트워크 접근 여부를 결정할 수 있다.
③ X — SSID는 무선 LAN을 식별하는 네트워크 이름이지 개별 장비의 인가 여부를 판별하는 식별값이 아니다. 틀린 부분은 SSID를 장비 인증기술로 본 점이며, 올바르게는 SSID는 접속 대상 무선 네트워크를 구분하는 식별자라고 해야 한다.
④ X — WEP는 공유 키를 이용하여 무선 구간의 접근과 통신을 보호하는 기술이므로 기관이 등록한 개별 장비인지를 MAC 주소처럼 직접 식별하지 않는다. 틀린 부분은 WEP를 개별 장비 인증기술로 본 점이며, 올바르게는 이 정책에는 허용된 MAC 주소를 대조하는 인증기술을 적용해야 한다.

오답 포인트

‘인증’이라는 공통 표현 때문에 ID/PW나 WEP를 고르기 쉽다. 그러나 문제의 결정적 조건은 ‘사용자가 누구인지는 확인하지 않음’과 ‘인가한 장비이면 접근 허용’이므로 사람의 계정이나 공유 키가 아니라 장비 식별값인 MAC 주소를 찾아야 한다.

NoteBase

다시 나오면 이렇게 판단

인증 대상을 먼저 구분한다. 사람의 신원이 기준이면 ID/PW, 장비 자체의 등록 여부가 기준이면 MAC 주소, 접속할 무선망의 구분이면 SSID, 공유 키를 통한 무선 구간 보호이면 WEP로 판단한다.

암기 포인트

사람은 ID/PW, 장비는 MAC 주소, 무선망 이름은 SSID, 공유 키 기반 무선 보호는 WEP이다.

NoteBase

문 20. 다음에서 설명하는 보안 장비는 무엇인가?

· 엔드포인트(Endpoint)가 처음 내부망 네트워크에 접근을 시도할 때 내부망에 피해가 없도록 엔드포인트에 일련의 보안정책을 적용하는 보안 솔루션이다.
· 내부 백신 설치여부, 컴퓨터 이름 등을 바탕으로 제한한다.

① IDS(Intrusion Detection System)
② IPS(Intrusion Prevention System)
③ NAC(Network Access Control)
④ NFS(Network File System)

정답 3번

출제 포인트

엔드포인트가 내부망에 접속하기 전에 보안 상태와 식별 정보를 검사하여 접근을 허용하거나 제한하는 NAC의 기능을 묻는 문제이다.

핵심 개념

NAC(Network Access Control)는 단말이 네트워크에 접속할 때 백신 설치 여부, 보안 정책 준수 여부, 컴퓨터 이름 등의 정보를 확인하여 접근을 허용·제한·격리하는 보안 솔루션이다.
IDS는 침입 탐지와 경보, IPS는 침입 탐지와 차단, NAC는 단말의 네트워크 접속 통제, NFS는 네트워크 파일 공유가 핵심이다.

선지별 해설

① X — IDS(Intrusion Detection System)는 네트워크나 시스템의 침입 징후를 탐지하여 관리자에게 알리는 장비이다. 틀린 부분은 '엔드포인트의 내부망 접근을 보안 상태에 따라 제한하는 장비'로 본 점이며, 올바르게는 NAC이다.
② X — IPS(Intrusion Prevention System)는 침입 트래픽을 탐지하고 실시간으로 차단하는 장비이다. 틀린 부분은 '백신 설치 여부나 컴퓨터 이름을 기준으로 단말의 접속을 통제하는 장비'로 본 점이며, 올바르게는 NAC이다.
③ O — NAC(Network Access Control)는 엔드포인트가 내부망에 접속하려 할 때 백신 설치 여부와 단말 식별 정보 등을 검사하고, 정책을 충족하지 못한 단말의 접근을 제한하거나 격리한다. 제시문의 설명과 일치한다.
④ X — NFS(Network File System)는 네트워크를 통해 원격 시스템의 파일을 공유하고 접근하게 하는 파일 시스템이다. 틀린 부분은 NFS를 네트워크 접근 보안 솔루션으로 본 점이며, 올바르게는 NAC이다.

NoteBase

오답 포인트

IDS와 IPS도 네트워크 보안 장비이므로 혼동하기 쉽다. 그러나 제시문의 핵심 표현은 '엔드포인트가 처음 내부망에 접근할 때'와 '백신 설치 여부·컴퓨터 이름을 바탕으로 제한'이다. 이는 공격 트래픽의 탐지나 차단이 아니라 단말의 접속 자격을 검사하는 NAC의 특징이다.

다시 나오면 이렇게 판단

침입을 발견해 알리면 IDS, 침입을 발견해 막으면 IPS, 단말의 보안 상태를 검사해 네트워크 접속을 허용·제한하면 NAC, 원격 파일을 공유하면 NFS로 판단한다.

암기 포인트

IDS는 탐지, IPS는 차단, NAC는 접속 통제, NFS는 파일 공유이다.

NoteBase