🥷

[취업폭격기 Zeromini 위클리 개념 정밀 타격 #35] [빈칸넣기문제]

📕 과목 : 네트워크보안

🔥 참고문제 : 개념폭격 자료 참고 #1

[취업폭격기 Zeromini 위클리 개념폭격 #1] (정보보안-네트워크보안)

https://zeromini-lab.com/blog/51/ 내용 참고

🌝 문제 수정 버전 : V 1.0

1. HTTPS 통신에서 대부분의 요소가 암호화되지만, 요청의 _____ 중 일부는 암호화되지 않습니다.
    - 답: 메타데이터
    - 해설: 요청의 URL, HTTP 메소드, 몇몇 HTTP 헤더 등이 암호화되지 않습니다.

2. 커버로스 프로토콜은 MIT에서 개발된 네트워크 인증 프로토콜로, 클라이언트와 서버 간의 안전한 인증을 제공합니다. 이 프로토콜은 신뢰할 수 있는 제 3 자인 _____를 사용하여 인증을 수행합니다.
    - 답: 키 분배 센터 (KDC)
    - 해설: 커버로스는 키 분배 센터를 사용하여 클라이언트와 서버 간의 인증을 수행합니다.
3. _____ 공격은 네트워크 트래픽을 도청하여 중요한 정보를 획득하는 공격 방법입니다.
    - 답: 스니핑
    - 해설: 스니핑 공격은 네트워크 상의 데이터를 가로채 중요 정보를 획득합니다.
4. OpenFlow 프로토콜은 _____의 핵심 프로토콜로, 네트워크의 제어 평면과 데이터 평면을 분리합니다.
    - 답: SDN (Software Defined Networking)
    - 해설: OpenFlow는 네트워크를 프로그래밍 가능하게 만드는 SDN의 핵심 프로토콜입니다.
5. SSL/TLS 공격 유형 중, 공격자가 통신을 중계하면서 암호화된 데이터를 복호화하거나 조작할 수 있는 공격은 _____ 공격입니다.
    - 답: 중간자
    - 해설: 중간자 공격에서 공격자는 통신을 중계하며 데이터를 복호화하거나 조작합니다.
6. POP3 프로토콜은 이메일 서버로부터 이메일을 다운로드하고, 이메일 클라이언트에서 이메일을 확인하는 데 사용되는 프로토콜입니다. 이 프로토콜은 이메일 서버와 클라이언트 간의 통신을 위한 _____로 동작합니다.
    - 답: 명령과 응답
    - 해설: POP3는 이메일 서버와 클라이언트 간의 명령과 응답을 통해 동작합니다.
7. IPv4 데이터그램의 'Flags' 필드는 _____와 관련이 있는 필드입니다.
    - 답: 단편화
    - 해설: 'Flags' 필드는 데이터그램의 단편화와 관련이 있습니다.
8. 네트워크 관리 기능 중 성능 관리는 네트워크를 감시하고 제어하는 기능으로, 시스템 성능을 측정하고, 지연 시간과 대역폭 사용률, _____ 등을 관리합니다.
    - 답: 패킷 처리율

- 해설: 성능 관리는 네트워크의 효과적인 실행을 보장하기 위해 다양한 메트릭을 관리합니다.

9. X.509(PKIX) 모델에서 종단 개체와 인증 기관 간의 관리 기능에는 등록, 키 쌍 복구, 키 쌍 갱신, _____ 등이 있습니다.
    - 답: 교차 인증
    - 해설: X.509 모델에서는 등록, 키 쌍 복구, 갱신, 교차 인증 등의 관리 기능이 있습니다.
10. 스미싱 공격을 예방하기 위해서는 보호되지 않은 무선 공유기의 사용을 피하고, 알 수 없는 출처의 앱 설치를 허용하지 않으며, _____을 설치하여 스마트폰의 보안 상태를 주기적으로 점검해야 합니다.
    - 답: 모바일 백신
    - 해설: 스미싱 공격 예방을 위해 모바일 백신 설치와 스마트폰 보안 점검이 중요합니다.
11. Firewall은 네트워크의 보안을 유지하기 위해 사용되는 장치 또는 소프트웨어로, 사전에 정의된 규칙에 따라 네트워크 트래픽을 _____합니다.
    - 답: 허용하거나 차단
    - 해설: 방화벽은 네트워크 트래픽을 허용하거나 차단하여 보안을 유지합니다.
12. IEEE 802.11i RSN의 동작 단계 중, 클라이언트와 액세스 포인트 간의 통신이 가능한지 확인하는 단계는 _____ 단계입니다.
    - 답: 탐색
    - 해설: IEEE 802.11i RSN의 탐색 단계에서는 클라이언트와 액세스 포인트간의 통신 가능성을 확인합니다.
13. SNMP에서 관리 대상 장치 내부 객체들에 대한 정보를 저장하는 저장소를 _____라고 합니다.
    - 답: MIB(Management Information Base)
    - 해설: SNMP에서 MIB는 네트워크 장치의 상태, 구성, 성능 등에 대한 정보를 저장합니다.
14. 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격은 _____ 공격입니다.
    - 답: ICMP 리다이렉트

- 해설: ICMP 리다이렉트 공격은 트래픽을 공격자에게 유도하여 네트워크 트래픽을 도청하거나 조작합니다.

15. 시저 암호는 각 문자를 알파벳 순서로 일정한 수만큼 이동시켜 암호화하는 방법입니다. 예를 들어, 평문 "STUDY"를 시저 암호로 암호화하면 암호문은 _____가 됩니다.
    - 답: "VWXGB"
    - 해설: 시저 암호는 각 문자를 알파벳 순서로 3칸 이동시켜 "STUDY"를 "VWXGB"로 암호화합니다.
16. SSL Handshake 프로토콜의 '서버 인증과 키 교환' 단계에서 인증서 메시지가 사용되지 않는 기법은 _____ 기법입니다.
    - 답: Anonymous DH
    - 해설: Anonymous DH 기법은 서버의 인증서를 사용하지 않으므로 중간자 공격에 취약합니다.
17. 전자 서명은 디지털 데이터에 첨부되어, 데이터의 무결성과 송신자의 신원을 확인할 수 있게 하는 기술입니다. 전자 서명은 송신자의 _____를 사용하여 생성됩니다.
    - 답: 개인 키
    - 해설: 전자 서명은 송신자의 개인 키를 사용하여 생성되며, 수신자는 공개 키로 검증합니다.
18. 네트워크 보안에서 IDS(Intrusion Detection System)와 IPS(Intrusion Prevention System)의 차이점은 IDS는 공격을 감지하고 경고를 발생시키지만, IPS는 비정상적인 행동이나 알려진 공격을 _____ 기능을 가집니다.
    - 답: 실시간으로 차단
    - 해설: IPS는 IDS의 기능에 더해 실시간으로 공격을 차단하는 기능을 가지고 있습니다.
19. 대칭키 암호화는 암호화와 복호화에 같은 키를 사용하는 반면, 비대칭키 암호화는 암호화와 복호화에 서로 다른 키인 _____를 사용합니다.
    - 답: 공개키와 개인키
    - 해설: 비대칭키 암호화는 암호화에 공개키를, 복호화에 개인키를 사용합니다.
20. 네트워크 보안에서 사용되는 '포트 스캐닝'은 네트워크에 연결된 컴퓨터의 특정 포트가 열려 있는지 확인하는 과정으로, 공격자가 시스템의 취약점을 찾아내는 데 사용될 수 있습니다. 열려 있는 포트를 통해 공격자는 시스템에 _____ 등의 공격을 시도할 수 있습니다.
    - 답: 접근하거나 서비스를 중단시키는

- 해설: 포트 스캐닝은 시스템의 취약점을 찾아내고, 열려 있는 포트를 통해 공격을 시도합니다.

21. 네트워크 보안에서 '피싱' 공격은 사용자를 속여 개인 정보를 획득하는 공격 방법으로, 공격자는 주로 이메일이나 웹사이트를 통해 가짜 메시지를 보내고, 이를 통해 사용자의 _____ 등을 획득합니다.
    - 답: 로그인 정보, 신용카드 정보
    - 해설: 피싱은 가짜 메시지를 통해 사용자의 개인 정보를 획득하는 공격 방법입니다.
22. 네트워크 보안에서 '인증'은 사용자, 시스템, 또는 서비스의 신원을 확인하는 과정으로, 일반적으로 사용자 이름과 비밀번호, _____, 바이오메트릭 데이터 등을 사용하여 수행됩니다.
    - 답: 디지털 인증서
    - 해설: 인증 과정은 사용자의 신원을 확인하기 위해 다양한 방법을 사용합니다.
23. 네트워크 보안에서 '암호화'는 정보를 안전하게 보호하기 위해 데이터를 읽을 수 없는 형태로 변환하는 과정입니다. 암호화된 데이터는 _____를 가진 사람만이 복호화하여 원래의 형태로 되돌릴 수 있습니다.
    - 답: 적절한 키
    - 해설: 암호화는 데이터를 보호하고, 데이터의 무결성을 유지하며, 데이터의 출처를 확인하는 데 사용됩니다.
24. 네트워크 보안에서 '방화벽'은 네트워크의 보안을 유지하기 위해 사용되는 장치 또는 소프트웨어로, 사전에 정의된 _____에 따라 네트워크 트래픽을 허용하거나 차단합니다.
    - 답: 규칙
    - 해설: 방화벽은 네트워크 내부와 외부 간의 통신을 제어하여, 외부로부터의 불필요하거나 위험한 접근을 차단하고, 내부 네트워크의 정보를 보호합니다.
25. IEEE 802.11i RSN의 동작 단계 중, 클라이언트와 액세스 포인트 간의 통신이 가능한지 확인하는 단계는 _____ 단계라고 합니다.
    - 답: 탐색 (discovery)
    - 해설: IEEE 802.11i RSN의 동작 단계는 탐색, 인증, 키 생성 및 분배, 안전 데이터 전송 단계를 포함합니다.