【시스템네트워크보안】

1. ARP 스푸핑(Spoofing) 공격은 ARP 캐시 테이블에 저장된 대응 관계를 조작해 수행하는 공격 방법이다. 다음에서 ARP 캐시 테이블에 저장되는 대응 관계가 가장 적절하게 연결된 것은?

- ① MAC 주소 - IP 주소 ② TCP 포트 - IP 주소
- ③ 도메인 이름 - IP 주소 ④ MAC 주소 - 도메인 이름

2. 다음 중 TCP/UDP 프로토콜을 사용하는 서비스에 대하여, <서비스명> <포트번호> <전송프로토콜>의 관계를 연결한 것으로 가장 적절하지 **않은** 것은?

	<서비스명>	<포트번호>	<전송프로토콜>
①	SMTP	25	TCP
②	DHCP	67,68	UDP
③	SSH	22	UDP
④	SSL	443	TCP

3. 다음 중 Unix 서버의 사용자 계정에 관련된 파일의 설명으로 가장 적절하지 **않은** 것은?

- ① /etc/passwd: 사용자 기본 정보 파일
- ② /etc/shadow: 암호화된 사용자 패스워드, 패스워드 정책이 포함된 파일
- ③ /etc/group: 그룹 기본 정보 파일
- ④ /etc/login.defs: 사용자 계정 생성 시 기본 정보를 가지고 있는 파일

4. 다음 중 TLS 1.3에 대한 설명으로 가장 적절하지 **않은** 것은?

- ① 0-RTT(Zero-Round Trip Time)이 추가되었다.
- ② 해시 알고리즘 중 MD5와 SHA-224가 사용되지 않는다.
- ③ 모든 핸드셰이크(Handshake) 메시지가 암호화된다.
- ④ RC4 알고리즘이 제거되었다.

5. 다음에서 설명하는 은닉전략(Concealment Strategy) 바이러스로 가장 적절한 것은?

- 감염시킬 때마다 변이가 일어난다.
- 변이가 일어날 때마다 자신을 완벽하게 새로 만들어서 탐지하기 어렵다.
- 모양만 변경하지 않고 동작도 변화시킨다.

- ① 암호화된 바이러스(Encrypted Virus)
- ② 스텔스 바이러스(Stealth Virus)
- ③ 폴리모픽 바이러스(Polymorphic Virus)
- ④ 메타모픽 바이러스(Metamorphic Virus)

6. 다음에서 sudo 명령에 대한 가장 적절한 것을 모두 고른 것은?

- ㉠ sudo 명령은 일반 사용자 계정을 root 계정으로 전환하기 위해 사용된다.
- ㉡ sudo 명령을 사용할 때 암호는 root 계정의 암호를 사용한다.
- ㉢ root 계정으로 실행 가능한 명령을 일반 사용자가 실행할 수 있게 해준다.
- ㉣ 사용자가 sudo 명령을 사용할 수 있도록 /etc/sudoers 파일에 권한을 설정한다.

- ① ㉠㉡ ② ㉠㉢㉣ ③ ㉢㉣ ④ ㉡㉢㉣

7. 다음과 같이 Linux에서 명령을 수행한 후, 새로 만들어지는 일반파일과 디렉터리파일의 접근권한을 8진수로 표현한 것으로 가장 적절한 것은?

```
umask 025
```

	일반파일	디렉터리파일
①	641	641
②	641	752
③	752	752
④	752	641

8. VPN(Virtual Private Network)에 대한 설명으로 가장 적절하지 **않은** 것은?

- ① 공중망을 이용하여 사설망과 같은 효과를 얻는다.
- ② 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.
- ③ VPN 구현 기술에는 터널링, 암호화, 인증, 접근제어 등이 있다.
- ④ IPsec은 VPN 터널의 업계 표준 프로토콜로 강력한 사용자 인증과 암호화를 제공하는 OSI 2계층 프로토콜이다.

9. Linux의 네트워크 관련 명령 <보기 1>과 설명 <보기 2>를 가장 적절하게 연결한 것은?

————— <보기 1> —————

(가) ifconfig	(나) nslookup
(다) route	(라) netstat

————— <보기 2> —————

- ㉠ DNS(Domain Name Service) 서버에 질의하기
- ㉡ 네트워크 인터페이스 설정하기
- ㉢ 네트워크의 상태정보를 출력하기
- ㉣ 기본 게이트웨이 설정하기

	(가)	(나)	(다)	(라)
①	㉠	㉡	㉢	㉣
②	㉡	㉠	㉣	㉢
③	㉠	㉡	㉣	㉢
④	㉡	㉠	㉢	㉣

10. 다음에 설명하는 메모리 위법행위(Memory Corruption)의 취약점으로 가장 적절한 것은?

- 브라우저에서 많이 발생하는 취약점으로, 반납된 포인터를 사용할 때 발생한다.
- 자바스크립트, 파일 로딩 등으로 힙 메모리를 조작할 수 있는 상황에서 공격이 가능하다.

- ① Heap Buffer Overflow ② Stack Overflow
- ③ Use-After-Free ④ Double Free

11. 다음 중 IPv6에 대한 설명으로 가장 적절하지 **않은** 것은?

- ① 주소의 길이는 64비트이다.
- ② 주소할당은 네트워크 규모, 단말기 수에 따라 순차적으로 할당한다.
- ③ 주소의 개수는 2¹²⁸개이다.
- ④ 전달 방식에는 유니캐스트, 애니캐스트 등이 있다.

12. 침입탐지시스템(Intrusion Detection System)에 대한 기능으로 가장 적절한 것을 모두 고른 것은?

- ㉠ 네트워크를 실시간 감시하는 기능
- ㉡ 네트워크에 유해한 트래픽을 탐지하고 차단하는 기능
- ㉢ 네트워크를 통한 웹 공격, 바이러스 공격 등을 탐지하고 차단하는 기능
- ㉣ 침입 분석 및 사용자 리포트 기능

- ① ㉠㉡ ② ㉠㉢ ③ ㉡㉢ ④ ㉢㉣

13. 프락시 방화벽(Proxy Firewall)의 장점으로 가장 적절하지 않은 것은?

- ① 트래픽 처리 성능이 향상된다.
- ② 가능하면 응용프로그램 계층까지 전체적으로 패킷 안의 정보를 검사한다.
- ③ 패킷 필터링보다 좋은 성능의 보안을 제공한다.
- ④ 보호되는 시스템과 보호되지 않는 시스템 사이의 연결을 차단시킨다.

14. NAT(Network Address Translation)는 내부 네트워크의 사설 IP 주소를 외부 네트워크의 공인 IP 주소로 변환 또는 역변환하는 기술을 의미한다. 다음 중 NAT의 장점으로 가장 적절하지 않은 것은?

- ① 공중망에 접속 유연성 제공
- ② 내부망 주소 방식에 대한 일관성 제공
- ③ 네트워크 보안 기능 제공
- ④ 네트워크 속도 향상

15. 다음과 같이 방화벽을 관리하는 iptables 명령을 이용하여 특정한 조건이 충족될 때만 포트가 동적으로 오픈되도록 하는 기술로 가장 적절한 것은?

```
iptables -A INPUT -p icmp --icmp-type echo-request -m recent --set --name PING
iptables -A INPUT -p tcp --dport 22 -m recent --rcheck --seconds 5 --name PING -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 --dport 22 -j DROP
```

- ① 포트 포워딩(Port Forwarding)
- ② 포트 노킹(Port Knocking)
- ③ 포트 예약(Port Reservation)
- ④ 포트 할당(Port Assignment)

16. Windows 레지스트리 루트키에 대한 설명으로 가장 적절한 것은?

- ① HKEY_CURRENT_USER: 컴퓨터에서 모든 계정에 관한 정보를 저장한다.
- ② HKEY_USERS: 현재 로그인된 사용자와 관련된 데이터를 저장한다.
- ③ HKEY_CLASSES_ROOT: 시스템 관련 정보를 저장한다.
- ④ HKEY_CURRENT_CONFIG: 현재 하드웨어 프로필에 관한 일부 정보를 저장한다.

17. 다음에서 설명하고 있는 전자우편(e-mail) 보안 프로토콜로 가장 적절한 것은?

- 전자우편 에이전트 간 분배단계에서 스팸을 처리하는데 사용할 수 있다.
- 수신측에서 MDA(Message Delivery Agent)는 DNS(Domain Name Service)를 이용해 해당 공개키를 가져와 서명 검증을 할 수 있다.
- 클라이언트 프로그램(MUA: Message User Agent)에서 구현되지 않기 때문에 사용자에게 투명하게 동작한다.

- ① DKIM(DomainKeys Identified Mail)
- ② IMAP(Internet Mail Access Protocol)
- ③ PGP(Pretty Good Privacy)
- ④ S/MIME(Secure/Multipurpose Internet Mail Extension)

18. Windows 파일 시스템에는 FAT(File Allocation Table) 방식과 NTFS(New Technology File System) 방식이 있다. 다음에서 FAT 방식과 비교하여 NTFS 방식의 장점으로 가장 적절한 것을 모두 고른 것은?

- ㉠ 호환성 우수
- ㉡ 강력한 보안 기능
- ㉢ 자동 압축 및 안정성
- ㉣ 디스크의 효율적 사용

- ① ㉠㉡ ② ㉠㉢ ③ ㉠㉢㉣ ④ ㉡㉢㉣

19. 다음 중 Linux의 시스템 로그에 대한 설명으로 가장 적절하지 않은 것은?

- ① lastlog: 사용자의 IP 주소별로 가장 최근에 로그인한 시간, 접속 장소, 사용자 이름, IP 주소정보 등을 기록
- ② wtmp: 파일이 생성되는 순간부터 로그인/로그아웃 정보 기록
- ③ btmp: 시스템에 현재 로그인한 사용자에 대한 상태 정보 기록
- ④ syslog: 사용자 인증과 관련된 로그 및 커널, 데몬에서 생성된 모든 로그를 포함하여 기록

20. Windows 운영체제에서 감사정책은 어떤 로그를 기록할지 정의한 규칙을 말한다. 다음 감사정책의 설명으로 가장 적절하지 않은 것은?

- ① 로그인 이벤트 감사: 시스템 액세스 제어 목록(SACL)이 지정되어 있는 액티브 디렉터리(Active Directory) 개체에 접근하는 사용자에게 대한 감사 로그를 제공한다.
- ② 권한 사용 감사: 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
- ③ 계정 관리 감사: 신규 사용자, 그룹의 추가, 기존 사용자 그룹의 변경, 사용자의 활성화나 비활성화, 계정 패스워드 변경 등을 감사한다.
- ④ 정책 변경 감사: 사용자 권한 할당 정책, 감사 정책 또는 신뢰 정책의 변경과 관련된 사항을 로깅한다.