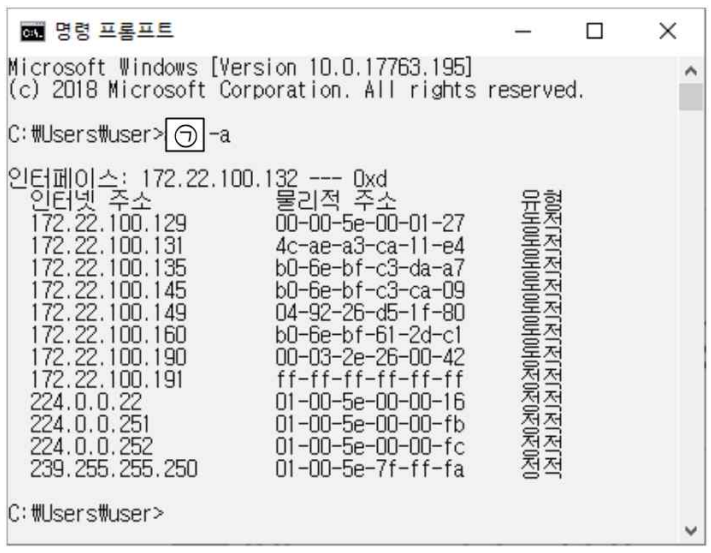
【시스템네트워크보안】

1. 다음 설명에 해당하는 것으로 가장 적절한 것은?

> 라우팅(routing)의 무한루프를 막기 위해 사용되는 것으로 라우터 하나를 지날 때마다 이 값이 1씩 줄어들고 목적지에 도착하기 전에 값이 0이 되면 해당 패킷은 폐기된다.

① HLEN(Header Length)
② TOS(Type Of Service)
③ TTL(Time To Live)
④ TLS(Transport Layer Security)

2. 다음 그림은 ㉠의 명령어를 실행한 결과이다. ㉠에 들어갈 명령어로 옳은 것은?



① netstat ② ipconfig
③ arp ④ ping

3. IPv6에 관한 설명으로 가장 적절하지 **않은** 것은?

① 기본 헤더의 길이는 40바이트이다.
② IPv4의 TTL 필드와 같은 목적으로 Hop Limit를 사용한다.
③ IPv4의 주소 32비트 길이를 4배 확장한 128비트 길이의 주소를 사용한다.
④ Traffic Class 필드는 20비트 길이로 응용서비스에 따라 차별화된 QoS를 제공한다.

4. 패스워드 크래킹(password cracking) 도구로 가장 적절하지 **않은** 것은?

① Striker ② John the Ripper
③ Pwdump ④ RainbowCrack

5. 방화벽(firewall)의 구축형태에 따른 장점으로 가장 적절하지 **않은** 것은?

① 스크리닝 라우터(screening router) 구조는 클라이언트와 서버의 환경변화 없이도 설치가 가능하다.
② 듀얼 홈드 게이트웨이(dual-homed gateway) 구조는 로그 정보 생성 및 관리가 용이하다.
③ 스크린드 호스트 게이트웨이(screened host gateway) 구조는 네트워크 계층과 응용 계층에서 방어하기 때문에 2단계 방어가 가능하다.
④ 스크린드 서브넷 게이트웨이(screened subnet gateway) 구조는 다른 방화벽의 구축 형태에 비해 설치와 관리가 쉽고 구축 비용이 적게 든다.

6. 다음 대응방법에 관련된 공격으로 가장 적절한 것은?

> • SetUID가 설정되어 있는 파일을 줄여야 한다.
> • 가능하면 임시파일을 생성하지 않는다.
> • 링크(link) 정보를 검사하여 비정상적인 링크를 제거한다.
> • 슈퍼유저(root) 소유의 중요한 파일에 관한 링크는 원천적으로 사용하지 못하게 통제한다.

① 레이스 컨디션(race condition) 공격
② 포맷 스트링(format string) 공격
③ 하트블리드(heartbleed) 공격
④ 시스템 자원 고갈(system resource exhaustion) 공격

7. 신뢰 플랫폼 모듈(TPM, Trusted Platform Module)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 운영체제가 단계적으로 인증된 절차를 거쳐 부팅되도록 한다.
② 휘발성 메모리 영역에 신뢰 플랫폼 모듈을 위한 신원, 상태 인자를 저장한다.
③ 난수 발생기, 암복호화 엔진, RSA(Rivest-Shamir-Adleman) 키 생성기 등을 포함한다.
④ 훼손방지를 위해 하드웨어칩으로 구현하는 것이 일반적이지만 소프트웨어로 구현하기도 한다.

8. 다음에서 시스템 취약점 점검 및 탐지 도구로 옳은 것만을 모두 고른 것은?

> ㉠ Netbus
> ㉡ Nmap(Network mapper)
> ㉢ SAINT(Security Administrator's Integrated Network Tool)
> ㉣ SATAN(Security Analysis Tool for Auditing Networks)

① ㉡㉢ ② ㉡㉣
③ ㉡㉢㉣ ④ ㉠㉡㉢㉣

9. 스푸핑(spoofing) 공격 유형에 관한 설명으로 가장 적절하지 **않은** 것은?

① IP 스푸핑 : 공격자가 정보를 얻거나 접근하기 위해 다른 컴퓨터의 IP 주소를 사용한다.
② E-Mail 스푸핑 : 이메일의 수신자를 위조하여 보내는 방식이다.
③ ARP 스푸핑 : MAC 테이블을 static으로 설정하여 막을 수 있다.
④ DNS 스푸핑 : 실제 DNS 서버보다 빨리 공격대상에게 DNS Response 패킷을 보내 공격대상이 잘못된 IP 주소로 접속하도록 유도하는 공격이다.

10. UNIX 시스템의 로그(log)에 관한 설명으로 가장 적절한 것은?

① dmesg는 원격지 접속 로그 등 인증과정을 거치는 모든 로그를 저장한다.
② history는 시스템 운영에 관련한 전반적인 로그로 /var/log/messages 파일에 저장한다.
③ utmp는 텍스트(text) 형태로 로그가 저장되며 w, who, users 명령어로 내용을 확인할 수 있다.
④ wtmp는 사용자들의 로그인과 로그아웃, 시스템 재부팅에 관한 정보를 담고 있으며 last 명령어로 내용을 확인할 수 있다.

11. 해커의 정보를 얻기 위한 시스템인 허니팟(honeypot)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 허니팟을 통과하는 패킷(packet)에 대해서 감시하지 않는다.
② 허니팟은 쉽게 해킹이 가능한 것처럼 취약해 보여야 한다.
③ 허니팟은 해커에게 쉽게 노출되어야 한다.
④ 허니팟은 시스템의 모든 구성 요소를 갖추고 있어야 한다.

12. 다음에서 버퍼 오버플로우(buffer overflow) 공격에 대응하는 방법으로 옳은 것만을 모두 고른 것은?

㉠ 스택 가드(stack guard) ㉡ 스택 쉴드(stack shield) ㉢ Non-Executable Stack ㉣ ASLR(Address Space Layout Randomization)

① ㉠㉡ ② ㉠㉡㉢
③ ㉡㉢㉣ ④ ㉠㉡㉢㉣

13. 다음 IDS(Intrusion Detection System)의 탐지 실행단계를 순서대로 나열한 것은?

㉠ 분석 및 탐지	㉡ 보고 및 대응
㉢ 데이터 수집	㉣ 데이터 가공 및 축약

① ㉢-㉣-㉠-㉡ ② ㉢-㉣-㉡-㉠
③ ㉠-㉡-㉢-㉣ ④ ㉠-㉡-㉣-㉢

14. 블루투스의 보안 위협 유형에 관한 설명으로 가장 적절하지 **않은** 것은?

① 블루프린팅(blueprinting) : 공격대상장치에 연결하여 임의의 파일을 삭제할 수 있다.
② 블루스나핑(bluesnarfing) : 공격대상장치에 있는 주소록이나 달력 등의 내용을 요청하여 열람하거나 취약한 임의의 파일에 접근할 수 있다.
③ 블루버깅(bluebugging) : 공격대상장치를 원격에서 연결하여 전화걸기, 불특정 번호로 SMS 보내기 등 임의의 동작을 실행시킬 수 있다.
④ 블루재킹(bluejacking) : 블루투스를 이용해 스팸 메시지를 익명으로 퍼트릴 수 있다.

15. 분산반사 서비스 거부(DRDoS, Distributed Reflection Denial of Service) 공격에 관한 설명으로 가장 적절하지 **않은** 것은?

① TCP에서 사용하는 3way-handshake의 취약점을 이용한다.
② 출발지의 IP 주소를 위조하는 공격이다.
③ 악성 봇(bot)의 감염을 통해서만 공격이 가능하다.
④ 공격트래픽이 수많은 반사서버를 경유하므로 역추적이 어렵다.

16. SecaaS(Security as a Service)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 인터넷을 사용해서 안전한 보안 서비스를 제공한다.
② IT 인프라 서비스를 제공하는 IaaS(Infrastructure as a Service)로 분류된다.
③ 서비스 제공자가 제공하는 보안 서비스 패키지이다.
④ 방화벽, 메일 보안, 신원 및 접근관리 등의 서비스를 제공한다.

17. 서버 보안용 점검 도구인 Tripwire에 관한 설명으로 가장 적절하지 **않은** 것은?

① 파일의 기밀성을 보장하는 것이 목적인 도구이다.
② 해커의 침입으로 인한 시스템 파일이나 디렉터리 변경을 쉽게 검출할 수 있다.
③ fcheck와 AIDE(Advanced Intrusion Detection Environment)도 비슷한 기능을 한다.
④ MD5(Message Digest 5), SHA(Secure Hash Algorithm), CRC-32(Cyclic Redundancy Check-32) 등의 해시함수를 제공한다.

18. 다음에서 설명하는 시스템으로 가장 적절한 것은?

빅데이터 분석 기술 등을 바탕으로 전자금융거래에 사용되는 단말기 정보, 접속정보, 거래내용 등의 정보들을 분석하여 이상금융거래를 탐지하고 차단하는 시스템을 의미한다. 정보수집 기능, 분석 및 탐지 기능, 대응 기능, 모니터링 및 감사 기능으로 구성되며, 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치할 수 있도록 지원하는 시스템을 말한다.

① NMS(Network Management System)
② IPS(Intrusion Prevention System)
③ IDS(Intrusion Detection System)
④ FDS(Fraud Detection System)

19. 다음 UNIX 시스템의 /etc/shadow 파일에 관한 설명으로 가장 적절하지 **않은** 것은?

police:5De3h9deY$5u78Fd~중략~T4e3rfG:13123:0:90:5:7:0:

① 패스워드(password) 만료 5일 전부터 사용자에게 경고한다.
② 사용자 패스워드는 SHA-512 일방향 해시 알고리즘이 적용되어 저장되었다.
③ 현재 사용 중인 패스워드를 변경하지 않고 사용할 수 있는 기간은 90일이다.
④ 패스워드가 마지막으로 변경된 날짜는 1970년 1월 1일을 기준으로 13,123일이 지났다.

20. 다음에서 설명하는 무선 LAN 프로토콜은?

IEEE 802.11n의 후속 버전으로 Wi-Fi 5라고 부르며, 정보를 최대 6.9Gbps의 속도로 전송하고 5GHz 주파수에서 높은 대역폭(80MHz~160MHz)을 지원한다.

① IEEE 802.11b ② IEEE 802.11g
③ IEEE 802.11i ④ IEEE 802.11ac