2022-국가직-9급-네트워크보안-나형-해설-곽후근

문 1. 네트워크 명령어에 대한 설명으로 옳지 않은 것은?

① hostname: 컴퓨터 이름을 확인한다.

② nslookup: DNS를 통해 도메인 이름을 검색한다.

③ ipconfig: 인터페이스에 설정된 라우팅 테이블을 검색한다.

④ ping: 컴퓨터의 네트워크 상태를 점검한다.

정답 체크

(3) route에 대한 설명이고, ipconfig는 일반적으로 네트워크 인터페이스의 IP 주소와 넷마스크의 설정 및 인터페이스의 활성화/비활성화 등을 위해 사용된다.

오답 체크

(1) 시스템의 이름을 확인하거나 바꿀때 사용하는 명령어이다.

(2) 인터넷 서버 관리자나 사용자가 호스트 이름을 입력하면 그 IP 주소를 알려 주는 프로그램이다(DNS를 이용). 그 반대의 경우에도 가능하다.

(4) 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다.

문 2. 다음에서 설명하는 네트워크 도구는?

○ IP 헤더에 있는 TTL의 특성을 이용한다. ○ TTL 값은 IP 패킷이 전송될 수 있는 최대 hop 수이다. ○ 최종 목적지까지의 라우터에 대한 경로 및 응답속도를 표시해 준다. ○ 특정 사이트와의 접속이 느릴 경우 네트워크의 어느 구간에서 느린지 확인할 수 있다.

① wireshark

② tcpdump

③ traceroute

④ netstat

정답 체크

(3) 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시해 준다.

오답 체크

(1) GUI 형태의 자유 및 오픈 소스 패킷 분석(캡처) 프로그램이다.

(2) CLI 형태의 패킷 분석(캡처) 프로그램이다.

(4) 유닉스, 리눅스, 윈도우에서 전송 제어 프로토콜, 라우팅 테이블, 수많은 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결을 보여주는 명령 줄 도구이다. 예를 들면, 현재 내 컴퓨터가 맺고 있는 TCP/UDP 연결 정보를 확인하기 위해 사용한다.

문 3. 비대칭키 암호화 알고리즘에서 수신자의 공개키로 데이터를 암호화하여 전송할 때 얻을 수 있는 보안성은?

① 가용성

② 인증

③ 부인방지

④ 기밀성

정답 체크

(4) 암호화를 수행하면 기밀성을 얻게 된다.

오답 체크

(1) 백업을 수행하면 가용성을 얻게 된다.

(2) MAC 또는 디지털 서명을 수행하면 인증(상호 인증, 서명자 인증)을 얻게 된다.

(3) 디지털 서명을 수행하면 부인방지를 얻게 된다.

문 4. TCP 포트의 개방 여부를 확인하기 위한 스텔스 스캔으로 옳지 않은 것은?

① FIN 스캔

② NULL 스캔

③ XMAS 스캔

④ TCP Open 스캔

정답 체크

(4) 연결을 맺음으로 로그를 남기게 된다(스텔스가 아니게 됨).

오답 체크

(1), (2), (3) 로그가 남지 않는 스텔스 스캔이다. 이외에도 TCP half Open 스캔이 존재한다.

문 5. 스위치 재밍(switch jamming)에 대한 설명으로 옳은 것은?

① 스위치 MAC 테이블의 저장 용량을 넘으면 더미 허브(dummy hub)처럼 브로드캐스트(broadcast) 한다.

② 방어대책은 게이트웨이 MAC 주소를 동적으로 설정한다.

③ 공격자는 클라이언트가 DNS 서버로 전송하는 DNS Query 패킷을 중간에 가로챈다.

④ MAC flooding은 스위치에 이상이 있을 때 자동으로 모든 보안 기능을 차단하는 것이다.

정답 체크

(1) 스위칭 허브를 더미 허브로 만들고, 더미 허브에서 브로드캐스트 되는 패킷을 스니핑한다.

오답 체크

(2) 정적으로 설정한다.

(3) DNS spoofing에 해당한다.

(4) MAC flooding은 장비가 가질 수 있는 MAC 테이블 용량이 넘치는 것을 의미한다.

문 6. 윈도시스템에서 다음과 같이 이더넷 인터페이스의 송수신 패킷 정보를 얻기 위한 netstat 명령어의 옵션은?

인터페이스 통계		
	받음	보냄
바이트	3879974308	172124956
유니캐스트 패킷	1098604	985784
비유니캐스트 패킷	11306144	94056
버림	0	0
오류	0	0
알 수 없는 프로토콜	0	

① netstat -an

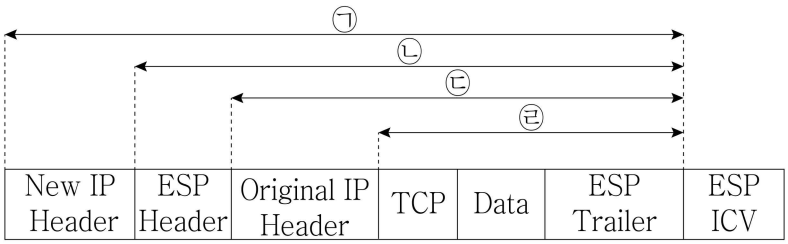
② netstat -e

③ netstat -r

④ netstat -s
정답 체크
(2) 유니캐스트 패킷에 대한 정보를 얻는다.
오답 체크
(1) 연결 상태 정보를 얻는다.
(3) 라우팅 정보를 얻는다.
(4) ICMP 정보를 얻는다.

문 7. SSL 프로토콜에 대한 설명으로 옳은 것은?
① ChangeCipherSpec 프로토콜은 오류와 비정상 상태를 알기 위해 사용한다.
② Handshake 프로토콜은 대기와 활성 상태 사이에서 이동되는 값들의 처리 과정을 규정한다.
③ Record 프로토콜은 기밀성과 메시지 무결성을 제공한다.
④ Alert 프로토콜은 암호 그룹 협의와 클라이언트와 서버 간 인증 정보를 교환하기 위해 사용한다.
정답 체크
(3) 압축한 단편과 메시지 인증 코드(상호 인증과 무결성 제공)를 합치고 그것을 대칭 암호로 암호화(기밀성 제공)를 수행하고, 암호화에는 CBC 모드를 이용한다.
오답 체크
(1) Alter 프로토콜에 해당한다.
(2) Handshake 프로토콜은 공유키를 생성하고 인증서를 교환한다. 공유키를 생성하는 것은 암호 통신을 행하기 위한 것이고(암호화), 인증서를 교환하는 것은 서로 상대를 인증하기 위한 것이다.
(4) Handshake 프로토콜에 해당한다.

문 8. IPSec의 ESP 터널 모드에서 암호화 범위로 옳은 것은?



① ㉠
② ㉡
③ ㉢
④ ㉣
정답 체크
(3) 터널 모드는 네트워크(Original IP Header), 전송(TCP), 응용(Data)을 보호한다.

문 9. TLS에 대한 설명으로 옳지 않은 것은?
① TLS는 SSL을 기반으로 만들어진 인터넷 표준이다.
② TLS의 의사난수 함수(pseudorandom function)는 데이터 확장 함수(data-expansion function)를 활용한다.
③ TLS의 의사난수 함수는 비밀(secret), 식별용 라벨(label), 종자(seed)를 입력받는다.

④ TLS의 마스터 비밀(master secret) 생성을 위해 데이터 확장 함수는 사전 마스터 비밀(pre-master secret), ‘master secret’ 문자, 2개의 임의의 수를 입력받는다.
정답 체크
(4) 사전 마스터 비밀과 2개의 임의의 수는 필요하지만 ‘master secret’ 문자는 필요하지 않다.
오답 체크
(1) SSL 3.0을 기반으로 한다.
(2) 데이터 확장 함수를 사용하면 필요할 때 알고리즘을 교체할 수 있다.
(3) pseudo-random 함수(PRF)는 secret, seed, label을 입력으로 받아서 임의의 길이의 결과값을 출력한다. PRF에서는 안전성을 보장하기 위해 두 개의 해쉬 알고리즘을 사용한다.

문 10. 부채널 공격(side channel attack)에 대한 설명으로 옳은 것은?
① 하드웨어적인 공격 기법이며, 전력분석, 시차분석, 전자파분석 등의 공격이 있다.
② 은닉 채널을 이용해 암호화 알고리즘이나 시스템 동작에서 발생하는 다양한 누수 정보를 획득한다.
③ 역어셈블러, 디버거를 이용해 소프트웨어의 오류 및 결함을 찾아 악용하는 공격이다.
④ 숨겨진 메시지를 사진이나 동영상 속에 부호화하는 스테가노그래피는 부채널 공격에 대응하기 위해 개발되었다.
정답 체크
(1) 알고리즘의 약점을 찾거나(암호 해독과는 다름) 무차별 공격을 하는 대신에 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.
오답 체크
(2) 은닉 채널(기본 채널에 기생하는 통신 채널)을 이용하지 않는다.
(3) 리버스 엔지니어링 공격이다.
(4) 암호화에 대응하기 위해 개발되었다(암호화를 하지 않고 숨김).

문 11. 디지털 포렌식(digital forensic)에서 ‘증거가 위조되거나 변조되지 않았다’는 것을 증명하는 원칙은?
① 무결성
② 신속성
③ 재현성
④ 정당성
정답 체크
(1) 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.
오답 체크
(2) 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(3) 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함을 의미한다.
(4) 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.

문 12. 대칭키 암호화 알고리즘으로 옳지 않은 것은?
① ARIA
② SEED

③ DES
④ ECC
정답 체크
(4) 공개키(비대칭키) 암호화 알고리즘이다.
오답 체크
(1), (2), (3) 대칭키 암호화 알고리즘이다.

문 13. 네트워크 서비스의 기본 포트 번호로 옳지 않은 것은?
① SMTP(Simple Message Transfer Protocol): 25
② DNS(Domain Name Service): 53
③ RPC(Remote Procedure Call): 111
④ SNMP(Simple Network Management Protocol): 143
정답 체크
(4) IMAP에 해당하고, SNMP는 161, 162번을 사용한다.
오답 체크
(1), (2), (3) 네트워크 서비스의 기본 포트 번호는 다음과 같다.

포트 번호	서비스	설명
20	FTP	• File Transfer Protocol (Data) • FTP 연결 시 실제로 데이터를 전송한다.
21	FTP	• File Transfer Protocol (Control) • FTP 연결 시 인증과 제어를 한다.
23, 22	Telnet, SSH	• 텔넷 서비스로, 원격지 서버의 실행창을 얻어낸다.
25	SMTP	• Simple Message Transfer Protocol • 메일을 보낼 때 사용한다.
53	DNS	• Domain Name Service • 이름을 해석하는 데 사용한다.
69	TFTP	• Trivial File Transfer Protocol • 인증이 존재하지 않는 단순한 파일 전송에 사용한다.
80	HTTP	• Hyper Text Transfer Protocol • 웹서비스를 제공한다.
110	POP3	• Post Office Protocol • 메일 서버로 전송된 메일을 읽을 때 사용한다.
111	RPC	• Sun의 Remote Procedure Call • 원격에서 서버의 프로세스를 실행할 수 있게 한다.
138	NetBIOS	• Network Basic Input Output Service • 윈도우에서 파일을 공유할 수 있게 한다.
143	IMAP	• Internet Message Access Protocol • POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
161, 162	SNMP	• Simple Network Management Protocol • 네트워크 관리와 모니터링을 위해 사용한다.

문 14. 침입탐지시스템(intrusion detection system)에 대한 설명으로 옳지 않은 것은?
① 침입탐지 유형에는 비정상행위 탐지(anomaly detection)와 오용 탐지(misuse detection) 등으로 구분된다.
② 비정상행위 탐지는 알려지지 않은 공격을 탐지하기에 효과적이지만 False Positive가 높아질 수 있다.
③ 오용 탐지는 알려진 공격 패턴을 기반으로 공격을 탐지하므로 알려지지 않은 공격 탐지에는 효과적이지 못하다.
④ 전문가 시스템 모델은 비정상행위 탐지에 널리 사용되는 기법이다.
정답 체크
(4) 오용탐지에 널리 사용된다. (비정상행위 탐지로 보는 견해도 있으나 기출에서 오용탐지로 나왔음)
오답 체크
(1) 비정상행위는 통계(정상에서 얼마나 벗어났는가?)에 기반하고, 오용탐지는 시그너처(웜이나 바이러스가 가지는 특정 문자열)에 기반한다.
(2) 정상적인 패킷을 공격 패킷으로 오인할 수 있다.
(3) False Negative가 높아진다(새로운 공격을 탐지하지 못함).

문 15. 다음에서 설명하는 서비스 거부(denial of service) 공격은?

○ ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용해 패킷을 확장 함으로써 서비스 거부 공격 수행
○ 다이렉트 브로드캐스트(direct broadcast) 악용

① 티어드롭 공격(teardrop attack)
② 스머프 공격(smurf attack)
③ 죽음의 핑 공격(ping of death attack)
④ SYN 플러딩 공격(SYN flooding attack)
정답 체크
(2) 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부(DDoS) 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
오답 체크
(1) 데이터의 송수신과정에서 데이터의 송신한계를 넘으면 MTU(1500byte) 조각으로 나누어 fragment number를 붙여 송신하고, 수신측에는 fragment 넘버로 재조합하여 분석한다. fragment 내의 나누어진 byte 정보인 fragmentation offset을 위조하여 offset을 중복되게 하거나 공간을 두면 수신측에서 재조합이 안 되어 다운이 되게 하는 공격이다. TCP에서는 순서 번호가 겹치는 공격이고, UDP에서는 프레그멘테이션 옵셋이 겹치는 공격이다.
(3) 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(4) 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.

문 16. 공격자가 TCP 세션 하이재킹(session hijacking)을 위해 대상 호스트에 첫 번째로 보내는 TCP 패킷 플래

그(flag)는?
① RST
② FIN
③ ACK
④ SYN
정답 체크
(1) ARP spoofing 후에 서버로 RST 패킷을 날린다.
오답 체크
(2), (4) TCP 세션 하이재킹 공격과 관련이 없다.
(3) RST을 보내고 다시 연결을 맺을 때 사용한다.

문 17. ICMP에 대한 설명으로 옳은 것은?
① 전송 계층에서의 오류 탐지를 위해 사용한다.
② 송신자의 패킷이 목적지에 도달하지 못했을 때 송신자는 ICMP Echo Reply 메시지를 수신한다.
③ TTL이 0이 되면 ICMP 시간초과(time exceeded) 오류 메시지가 발생한다.
④ UDP에 의해 전송된다.
정답 체크
(3) 패킷이 네트워크 사이에서 무한정 돌아가지 않도록 패킷을 처리할 때마다 TTL(Time to Live)을 감소시키다가 값이 '0'이 되면 보내는 메시지이다.
오답 체크
(1) 네트워크 계층에서 동작한다.
(2) Destination Unreachable 메시지를 수신한다.
(4) IP에 의해 전송된다.

문 18. IKE 키 결정 알고리즘의 특징에 대한 설명으로 옳지 않은 것은?
① 방해 공격을 방지하기 위해 비표(nonce)를 사용한다.
② 두 당사자가 군(group)을 협상할 수 있다.
③ Diffie-Hellman 공개키 값의 교환이 가능하다.
④ 중간자 공격을 방지하기 위해 Diffie-Hellman 교환을 인증한다.
정답 체크
(1) 쿠키를 사용한다.
오답 체크
(2) 보안 연관(SA, 어떤 암호화 알고리즘을 사용하고 키의 길이는 어떻게 할 것인지?)을 협상한다.
(3) IKE의 하부 프로토콜에서 Diffie-Hellman을 사용한다.
(4) Diffie-Hellman을 그냥 사용하면 중간자 공격을 당하므로 인증을 추가하여 중간자 공격을 방지한다.

문 19. IPSec의 보안 연관(security association)을 식별하기 위한 매개변수로 옳지 않은 것은?
① 보안 매개변수 색인(security parameters index)
② 발신지 IP 주소
③ 수신지 IP 주소
④ 보안 프로토콜 식별자(security protocol identifier)

정답 체크
(2) 발신지 IP 주소는 포함하지 않는다.
오답 체크
(1) SA를 나타내는 인덱스이다.
(3) 수신지 IP 주소를 가지고 해당 SA를 찾는다.
(4) AH, ESP를 나타낸다.

문 20. 다음의 설명에서 옳지 않은 것은?
① 스턱스넷(stuxnet): 사용자가 키보드로 입력하는 내용을 몰래 가로채어 기록한다.
② 랜섬웨어(ransomware): 시스템의 폴더 또는 파일 등을 암호화하여 금전을 요구한다.
③ 트로이 목마(trojan horse): 겉으로는 정상적인 프로그램으로 보이지만 악성코드가 숨겨져 있다.
④ 스파이웨어(spyware): 사용자 정보를 무단으로 수집하여 동의 없이 다른 곳으로 보낸다.
정답 체크
(1) 키로깅에 해당하고, 스턱스넷은 국가 및 산업의 중요 기반 시설을 제어하는 SCADA(Supervisory Control And Data Acquisition) 시스템을 대상으로 한 웜이다. 전파를 위해 윈도우 서버 서비스의 취약점을 이용해 공유 폴더를 공격했으며 윈도우 쉘 .lnk(바로가기) 취약점을 이용해 USB를, 윈도우 프린트 스풀러 서비스의 취약점인 공유 프린터를 전파 개체로 활용했다.
오답 체크
(2) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.
(3) 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.
(4) 자신의 컴퓨터에 설치된 시스템의 정보를 원격지의 특정한 서버에 주기적으로 보내는 프로그램이다.