Chapter 01

01. 해킹의 사전적 의미를 간단히 설명하시오.

타인의 컴퓨터 시스템에 무단 침입하여 데이터에 접속할 수 있는 권한을 얻는 것

02. 인공지능이라는 개념을 최초로 생각해낸 사람은? (1)

(1) 앨런 튜링 (2) 케빈 미트닉

(3) 켄 톰프슨 (4) 리처드 스톰먼

03. 1967년에 미국 국방부가 연구 기관과 국방 관련 사업체 등 관련 기관 사이의 정보 공유를 지원하기 위해 구축한 최초의 컴퓨터 연동망(네트워크)은? (2)

(1) TCP/IP (2) ARPA

(3) Telnet (4) TRM

04. 최초로 이메일이 전송된 시기는? (4)

(1) 1940년대 (2) 1950년대

(3) 1960년대 (4) 1970년대

05. 보안의 3대 요소는?

기밀성, 무결성, 가용성

06. 보안의 3대 요소 중 적절한 권한이 있는(인가된) 사용자만 정보에 접근할 수 있도록 허용하는 것은?

가용성

07. 보안 전문가가 갖춰야 할 기본 소양은?

윤리 의식

08. 보안 전문가가 갖춰야 할 기본 지식은?

운영체제, 네트워크, 프로그래밍, 서버, 보안 시스템, 모니터링 시스템, 암호 등 다양한 분야에 대한 전문성

Chapter 02

01. 다음 중 보안의 네 가지 인증 방법에 속하지 않는 것은? (2)

(1) 알고 있는 것 (2) 당신이 위치를 알고 있는 곳

(3) 가지고 있는 것 (4) 스스로의 모습

02. 유닉스 시스템에서 계정 목록을 확인할 수 있는 파일은? (3)

(1) /etc/envirionment (2) /etc/account

(3) /etc/passwd (4) /etc/shadow

03. 다음은 유닉스 시스템에서 확인한 각 계정별 정보다. 유효한(로그인이 가능한) 계정은? (2)

user1 : : 0 : 0 : root : /root : bin/bash

user2 :x: 0 : 0 : root : /root : bin/bash

user3 :x: 0 : 0 : root : /root : bin/false

user4 :x: 0 : 0 : root : /root : true

(1) user1 (2) user2

(3) user3 (4) user4

04. 세션에 대해 설명하시오.

세션은 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속을 의미

05. 어떤 사용자가 인증 절차를 거쳐 시스템에 접근하는 데 성공했다. 얼마 후 같은 아이디로 시스템에 접근하는 사용자가 처음 인증에 성공한 그 사용자인지 확인하기 위해 지속적으로 재인증을 수행하는 방법은 (지속적인 인증)이라고 한다.

06. 다음 중 주요 관리자 인터페이스와 서비스 포트가 잘못 연결된 것은? (1)

(1) xdmcp: 5500 (2) telnet: 23

(3) 윈도우 터미널 서비스: 3389 (4) ssh: 22

07. 네트워크에서 접근 제어의 가장 일반적인 수단은? (2)

(1) 클라이언트의 MAC 주소를 통한 접근 제어

(2) 클라이언트의 IP를 통한 접근 제어

(3) 클라이언트의 포트를 통한 접근 제어

(4) 클라이언트의 호스트 이름을 통한 접근 제어

08. NTFS 파일 시스템의 윈도우에서 파일 및 디렉터리에 대한 권한을 부여할 때 올바른 규칙이 아닌 것은? (4)

(1) NTFS 접근 권한이 누적된다. (2) 파일 접근 권한이 디렉터리 접근 권한보다 우선한다.

(3) ‘허용’보다’ ‘거부’가 우선한다. (4) 디렉터리 접근 권한이 파일 접근 권한보다 우선한다.

09. 유닉스 파일의 소유자에게만 읽기와 쓰기 권한이 있는 경우는? (1)

(1) rwxr—r—1 root root 312 Nov 30 13:05 listner.ora

(2) r-xrw-r—1 root root 312 Nov 30 13:05 listner.ora

(3) rwxrw-rw-1 root root 312 Nov 30 13:05 listner.ora

(4) rwxr—r-w 1 root root 312 Nov 30 13:05 listner.ora

10. 다음 중 권한 관리를 위한 DCL이 아닌 것은? (2)

(1) GRANT (2) SELECT

(3) DENY (4) REVOKE

11. 뷰에 대해 간단히 설명하시오.

뷰는 참조 테이블의 각 열에 대해 사용자의 권한을 설정하는 것이 불편해서 만든 가상 테이블

12. 현재 로그인한 사용자의 아이디, 사용자 프로세스, 실행 레벨, 로그인 종류 등이 기록되는 로그 파일은? (4)

(1) lastlog (2) sulog

(3) messages (4) utmp

13. 리눅스 시스템의 TCP Wrapper에서 제공하는 기능이 아닌 것은? (1)

(1) 로깅 (2) 포트 접근 통제

(3) IP 기반 접근 통제 (4) 네트워크 서비스 기반 통제

14. 다음 설명 중 옳지 않은 것은? (2)

(1) 리눅스 시스템에서는 계정 목록을 /etc/passwd 파일에 저장하고 있다

(2) 일반 사용자의 사용자 번호(UID, UserID)는 0번으로 부여받게 된다.

(3) 디렉터리의 권한은 특수 권한, 파일 소유자 권한, 그룹 권한, 일반(Others) 권한으로 구분된다.

(4) 접근 권한이 rwxr-xr-x인 경우 고유한 숫자로 표기하면 755가 된다.

15. Authentication(인증), Authorization(인가), Accounting)에 대해 각각 설명하시오.

Authentication(인증): 자신의 신원을 시스템에 증명하는 과정

Authorization(인가): 신원이 확인되어 인증받은 사람이 출입문에 들어가도록 허락하는 과정

Accounting: 로그인 했을 때 시스템이 이에 대한 기록을 남기는 활동

16. 다음 로그에 대해 각 항목을 매핑하시오.

2021-06-03 08:53:12 192.168.137.128

GET/XSS/GetCookie.asp?cookie=ASPSESSIONIDQQ CAQDDA 80 - 192.168.137.1

Mozila/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;) 200 0 0 225

날짜와 시간: 2021-06-03 08:53:12

서버 IP: 192.168.137.128

HTTP 접근 방법과 접근 URL: GET/XSS/GetCookie.asp?cookie=ASPSESSIONIDQQ CAQDDA

서버 포트: 80

클라이언트 IP: 192.168.137.1

클라이언트의 웹 브라우저: Mozila/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;)

실행 결과 코드: 200(OK)

서버에서 클라이언트로 전송한 데이터의 크기: 0

클라이언트에서 서버로 전송한 데이터의 크기: 0

처리 소요 시간: 255ms

17. 리눅스에서 관리하는 주요 로그 파일에 대한 설명으로 옳지 않은 것은? (4)

(1) /var/log/utmp: 현재 로그인한 사용자의 아이디, 사용자 프로세스, 실행 레벨, 로그인 종류 등을 기록

(2) /var/log/syslog: 시스템 운영과 관련된 전반적인 로그

(3) /var/log/secure: 시스템의 접속에 관한 로그로 언제/누가/어디의 정보를 포함

(4) /var/log/stmp: 메일 송수신에 관한 로그

18. Telnet 보안에 대한 설명으로 틀린 것은?

(1) TELNET 세션은 암호화 및 무결성 검사를 지원하지 않는다.

(2) SSH(Secure Shell)는 암호화를 하지 않는다

(3) 패스워드가 암호화되어 있지 않아 스니퍼를 이용하여 제 3자에게 노출될 수 있다.

(4) UNIX 시스템에서 해커가 in.telnetd를 수정하여 클라이언트의 특정 터미널 종류에 대해 인증 과정 없이 셸을 부여할 수도 있다.

19. 응용 프로그램 자체에 존재하는 취약점을 제거하는 방법은? (1)

(1) 패치 (2) 접근 제어

(3) 권한 관리 (4) 무결성 점검

20. RIM이 만든 모바일 운영체제로 메시지와 이메일 전송 기능 및 보안에 초점을 둔 모바일 운영체제는? (1)

(1) 블랙베리 OS (2) iOS

(3) 안드로이드 (4) 윈도우 CE

21. 다음 중 iOS의 특징으로 적절하지 않은 것은? (3)

(1) 응용 프로그램이 샌드박스 안에서 실행된다.

(2) 시스템 소프트웨어 개인화가 가능하다.

(3) 리눅스 커널(2.6.25)을 기반으로 만들어진 모바일 운영체제다.

(4) 모든 앱에 대해 코드 무결성 사인을 등록한다.

22. 애플이 자신의 CA를 통해 각각의 응용 프로그램을 서명하여 배포하는 반면, 안드로이드는 (개발자)가 서명하도록 하고 있다.

23. 애플이 응용 프로그램의 실행을 통제하기 위해 가상 머신 안에서 실행하듯 응용 프로그램을 원래 운영체제와 완전히 독립되게 실행하는 것을 무엇이라고 하는가?

샌드박스(sandbox)

24. 서비스 발견 프로토콜(SDP)을 통해 장치를 검색하고 모델을 확인하는 블루투스 공격은? (1)

(1) 블루프린팅 (2) 블루스나프

(3) 블루버그 (4) 블루잼

Chapter 03

01. TCP/IP의 4계층에 해당하지 않는 것은? (4)

(1) 인터넷 계층 (2) 전송 계층

(3) 응용 계층 (4) 물리 계층

02. MAC 주소는 무엇으로 이루어져 있는가? (3)

(1) 6개의 16진수 (2) 12개의 8진수

(3) 12개의 16진수 (4) 6개의 8진수

03. 공인 IP 주소로 가장 많은 호스트를 구성할 수 있는 네트워크는? (1)

(1) A 클래스 (2) B 클래스

(3) C 클래스 (4) D 클래스

04. 다음 중 네트워크 서비스와 포트가 잘못 연결된 것은? (4)

(1) FTP: 21 (2) DNS: 53

(3) HTTP: 80 (4) SMTP: 63

05. 3-웨이 핸드셰이킹에 대해 설명하시오.

TCP에서 가상 경로를 설정할 때 연결을 설정하는 과정을 말한다.

06. SYN 패킷만 보내어 서버를 점유함으로써 다른 사용자가 서버를 사용할 수 없게 하는 공격은? (1)

(1) SYN 플러딩 공격 (2) 랜드 공격

(3) 분산 서비스 거부 공격 (4) 스머프 공격

07. 다음 중 랜드 공격의 출발지 주소와 목적지 주소가 바르게 묶인 것은? (3)

[출발지 주소] [목적지 주소]

(1) 공격 대상의 클라이언트 IP 주소 공격 대상의 서버 IP 주소

(2) 공격 대상의 서버 IP 주소 공격 대상의 클라이언트 IP 주소

(3) 공격 대상의 서버 IP 주소 공격 대상의 서버 IP 주소

(4) 공격자의 IP 주소 공격 대상의 서버 IP 주소

08. 스머프 공격은 ICMP echo request를 이용하는 것이다. 이 echo request 패킷을 에이전트에 뿌리기 위해 라우터에서 지원해야 하는 것은?

다이렉트 브로드캐스트

09. 프러미스큐어스 모드에 대해 설명하시오.

스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하기 때문에 데이터 링크 계층과 네트워크 계층의 정보를 이용한 필터링은 방해물이다. 이때, 두 계층의 필터링을 해제하는 랜 카드의 모드를 말한다.

10. 스위칭 환경에서 스니핑을 수행하기 위한 공격이 아닌 것은? (3)

(1) ARP 스푸핑 (2) ICMP 리다이렉트

(3) IP 스푸핑 (4) 스위치 재밍

11. ARP 스푸핑은 몇 계층 공격에 해당하는가? (2)

(1) 1계층 (2) 2계층

(3) 3계층 (4) 4계층

12. IP 스푸핑 공격을 수행하기 위해 공격 대상이 사용하고 있어야 하는 것은? (2)

(1) SSO (2) 트러스트

(3) DRM (4) 웹 서비스

13. 스위칭 환경에서 스니핑을 하기 위한 공격과 거리가 먼 것은? (1)

(1) DNS Spoofing (2) ARP Broadcast

(3) ARP Jamming (4) Switch Jamming

14. 이메일과 관련된 프로토콜이 아닌 것은? (2)

(1) SMTP (2) SNMP

(3) POP3 (4) IMAP

15. 다음 중 무선 랜 구축 시 보안 고려 사항으로 가장 적합하지 않은 선택은? (4)

(1) SSID를 숨김 모드로 사용

(2) 관리자용 초기 ID/Password 변경

(3) 무선 단말기의 MAC 주소 인증 수행

(4) 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

16. DNS 정보를 요청한 클라이언트 측면에서 DNS 스푸핑이 가능한 가장 큰 요인을 설명하시오.

공격자는 로컬에 존재하므로 지리적으로 DNS 서버보다 가깝다. 따라서 DNS 서버가 올바른 DNS response 패킷을 보내주기 전에 클라이언트에 위조된 DNS response 패킷을 보낼 수 있다.

17. 세션 하이재킹을 하기 위해 서버 측에 최초로 보내는 TCP 패킷은? (2)

(1) SYN (2) RST

(3) FIN (4) ACK

18. 다음 중 무선 랜 보안 시 확인할 사항이 아닌 것은?

(1) SSID 브로드캐스팅 허용 (2) WEP 키 설정

(3) WPA-PSK 키 설정 (4) 802.1x 솔루션 도입

Chapter 04

01. 다음 중 최초의 네트워크는? (3)

(1) TCP/IP (2) WWW

(3) ARPA (4) 프레임 릴레이

02. 다음과 같이 URL을 통해 요청 데이터에 대한 인수를 전송하는 HTTP Request 방식은? (1)

[www.wishfree.or.kr/list.php?page=1&search=test](http://www.wishfree.or.kr/list.php?page=1&search=test)

(1) GET 방식 (2) POST 방식

(3) PUT 방식 (4) HEAD 방식

03. 다음 중 동적인 웹 페이지를 위한 서버 측 웹 스크립트 언어가 아닌 것은?

(1) JSP (2) PHP

(3) ASP (4) 자바스크립트

04. 구글에서 특정 도메인이 들어 있는 사이트에 대한 정보를 수집할 때 사용하는 검색 엔진은? (2)

(1) inurl (2) site

(3) type (4) filetype

05. 구글 검색 엔진에서 검색할 수 없도록 하기 위해 만드는 파일은? (2)

(1) forbidden.txt (2) robots.txt

(3) search.txt (4) deny.txt

* 06. SQL 삽입 공격이 가능한 경우에 대해 간단히 설명하시오.

07. 다음 중 SQL 삽입 공격에 쓸 수 있는 특수 문자열이 아닌 것은? (2)

(1) ‘ or ‘’=’-- (2) ‘ or ‘1’=’

(3) ‘ or ‘1’=’1 (4) ‘ or ‘’=’

* 08. 웹 서버의 세션 관리 측면에서 사용자 데이터를 이용한 인증으로 인해 발생할 수 있는 문제점을 간단히 설명하시오.

09. 웹 사이트에서 각각의 개인을 구별하기 위해 클라이언트에 저장해두는 것은? (1)

(1) 쿠키 (2) 식별자

(3) 비스켓 (4) 아이디

- 10. XSS 취약점 공격을 수행하는 단계를 순서대로 나열하시오.

(ㄱ) 공격자가 작성해둔 XSS 코드에 웹 서비스 사용자가 접근한다.

(ㄴ) 임의의 XSS 취약점이 존재하는 서버에 XSS 코드를 작성하여 저장한다.

(ㄷ) XSS 코드가 실행된 결과는 공격자에게 전달되고 공격자는 공격을 종료한다.

(ㄹ) 사용자 시스템에서 XSS 코드가 실행된다.

(ㅁ) 웹 서버는 사용자가 접근한 XSS 코드가 포함된 게시판의 글을 전달한다.

11. 파일 다운로드 시 디렉터리를 탐색하여 파일을 다운로드하는 것을 막기 위해 필터링해야 하는 문자열은? (1)

(1) .. (2) space

(3) ; (4) “

12. 웹 취약점 탐색 시 파일을 다운로드하기 위한 download.jsp 파일을 확인했다. 이 파일은 다음과 같은 형태로 동작한다.

http://www.wishfree.com/board/download.jsp?filename=사업계획.hwp

이 download.jsp 파일을 이용하여 시스템에 존재하는 /etc/passwd 파일을 다운로드하기 위한 URL을 완성하시오. (유닉스 서버이며, 서버에서 ‘사업계획.hwp’의 위치는 ‘/web/htdocs/webpage/upload/사업계획.hwp’이다.)

http://www.wishfree.com/board/download.jsp?filename=( ../../../etc/passwd)

13. 파일 목록을 열람할 수 있는 취약점은? (3)

(1) 파일 업로드 (2) 디렉터리 탐색

(3) 디렉터리 리스팅 (4) 파일 다운로드

* 14. 리버스 텔넷에 대해 간단히 설명하시오.

15. 다음 중 웹 취약점을 보완하는 방안으로 적절하지 않은 것은? (3)

(1) 특수 문자 필터링 (2) 서버 통제 적용

(3) 클라이언트 통제 적용 (4) 지속적인 세션 관리

16. 다음 중 CSRF 취약점의 특징이 아닌 것은? (4)

(1) 특정 소수가 아닌 불특정 다수를 대상으로 한다.

(2) 원래 의도된 기능이 아닌, 데이터 변경, 삭제 등이 가능해진다.

(3) XSS에서 진보한 공격이라고 보는 의견이 있다.

(4) XSS는 서버에서, CSRF는 클라이언트에서 악성 코드가 실행된다.

17. HTTP의 요청 메서드가 아닌 것은? (3)

(1) GET (2) POST

(3) PUSH (4) PUT

18. 다음에서 설명하는 웹 공격 기법은? (4)

게시판의 글에 원본과 함께 악성코드를 삽입하여, 글을 읽을 경우 악성 코드가 실행되도록 해서 클라이언트의 정보를 유출하는 클라이언트에 대한 공격 기법

(1) SQL Injection 공격 (2) 부적절한 파라미터 조작 공격

(3) 버퍼 오버플로 공격 (4) XSS(Cross Site Scripting) 공격