

정보시스템 보안

1. 프로그램이 실행될 때마다 해당 프로그램이 사용하는 메모리 주소를 무작위로 배치하여 공격 대상 프로그램이 사용하는 메모리 주소를 추측하기 어렵게 만드는 리눅스 운영체제의 기능은?

① DLL
② Canary
③ ASLR
④ Packing

2. 어떠한 작업을 주기적으로 실행시키기 위한 리눅스 명령어는?

① wc
② ps
③ df
④ crontab

3. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

리눅스에는 사용자의 비밀번호를 지정하거나 변경할 때 쓰이는 (가) 명령어가 있다. 이 명령어는 사용자의 비밀번호가 저장된 (나) 파일에 접근하여 기존 비밀번호를 새로 입력한 값으로 변경하는 기능을 한다. (가) 명령어를 일반 사용자가 실행하였다고 하더라도, 해당 프로세스가 관리자 계정만 접근권한이 있는 파일에 접근하여 비밀번호를 바꾸는 것이 가능한 이유는 (가) 명령어에 설정된 (다) 때문이다. 일반 사용자가 (다)가 설정된 (가) 명령어를 실행하면 해당 프로세스는 일시적으로 파일 소유자인 관리자(root)의 권한을 얻게 되어 관리자만 접근할 수 있는 (나) 파일에 접근하여 해당 사용자의 비밀번호를 수정할 수 있다.

(가)

(나)

(다)

① passwrd /etc/shadow SetUID
② passwrd /etc/passwd SetRID
③ passwd /etc/shadow SetUID
④ passwd /etc/shadow SetRID

4. 다음과 같이 시스템에 설정된 umask 값이 '022'인 경우, 파일(file1)을 생성하였을 때 생성된 파일의 접근권한은?

```
[root@security ~]# umask
022
[root@security ~]# touch file1
```

① -rwxr-xr-x
② -r-xrwxrwx
③ -rw-r--r--
④ -rw-----

5. 유닉스/리눅스 시스템의 로그 파일에 대한 설명으로 옳지 않은 것은?
- ① utmp 로그는 특정 시간에 로그인한 사용자의 정보를 텍스트 형태로 기록한다.
② wtmp 로그는 사용자의 로그인, 로그아웃, 시스템 재부팅 정보를 바이너리 형태로 기록한다.
③ su 로그는 su 명령어 수행에 따른 권한 변경 시도 및 변경 정보를 텍스트 형태로 기록한다.
④ pacct 로그는 시스템에 로그인한 모든 사용자가 수행한 프로그램의 정보를 바이너리 형태로 기록한다.
6. 동일한 네트워크에 있는 DHCP 서버와 클라이언트 간의 동작 과정을 순서대로 나열한 것은?

(가) 서버는 UDP 목적지 포트 번호 68, 발신지 포트 번호 67로 지정한 뒤, 유니캐스트 메시지나 브로드캐스트 메시지를 클라이언트에 전송
(나) UDP 사용자 데이터그램(user datagram)으로 캡슐화 이후, IP 데이터그램으로 캡슐화
(다) DHCP 서버는 UDP 포트 번호 67에 수동 개방(passive open) 명령을 수행
(라) 부팅된 클라이언트는 포트 번호 68에 능동 개방(active open) 명령을 수행

① (다) → (나) → (라) → (가)
② (다) → (라) → (나) → (가)
③ (라) → (다) → (가) → (나)
④ (라) → (다) → (나) → (가)

7. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

○ (가) 은 블루투스 공격 장치의 검색 활동을 뜻한다.
○ (나) 은 블루투스의 취약점을 이용하여 블루투스 기기의 정보에 접근하는 공격이다.
○ (다) 은 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다.

(가)

(나)

(다)

① 블루재킹(Bluejacking) 블루스나핑(Bluesnarfing) 블루프린팅(Blueprinting)
② 블루프린팅 블루스나핑 블루재킹
③ 블루스나핑 블루프린팅 블루버깅(Bluebugging)
④ 블루프린팅 블루스나핑 블루버깅

8. (가)에 들어갈 용어로 옳은 것은?

x86계열 32-bit CPU 환경에서, 구동 중인 프로세스가 사용하는 메모리 영역 중 스택 영역 관리에 사용되는 주요 레지스터는 EIP, (가), ESP가 있다. 스택 영역에는 함수 호출 시 전달되는 파라미터, 함수 실행 중 할당되는 지역변수, 함수 종료 시 되돌아갈 리턴 주소 등이 저장된다. 파라미터 및 지역변수는 (가)를 기준으로 오프셋 값을 설정하여 접근할 수 있다.

① ESI ② EAX
③ ECX ④ EBP

9. (가)에 들어갈 용어로 옳은 것은?

- (가) 은(는) 보안 관리자나 보안 시스템의 탐지를 피하면서 시스템을 제어하기 위해 공격의 의도로 설치되는 악성파일로, 보통 운영체제의 합법적인 명령어처럼 모아 놓은 것을 말한다.
- (가) 은(는) 공격자의 파일, 디렉터리 및 프로세스를 숨기는 것을 제외하고 합법적인 명령어처럼 동작한다.

- ① 랜섬웨어 ② 키로거
③ 워프 ④ 루트킷

10. AAA에 대한 설명으로 옳지 않은 것은?

- ① Authentication은 자신의 신원을 시스템에 증명하는 과정을 의미한다.
- ② Authorization은 지문 인식 시스템에 손가락을 댈 때 지문 자체를 의미한다.
- ③ Accounting은 시스템에 접근한 사용자 추적에 활용될 수 있다.
- ④ Accounting은 로그인했을 때 시스템이 이에 대한 기록을 남기는 활동을 의미한다.

11. 전자메일 시스템에서 송신 부인방지 기능을 위해 적용하는 기술은?

- ① 전자 서명(digital signature)
- ② 대칭키 암호화(symmetric encryption)
- ③ 앨리어스(alias)
- ④ 커버로스(Kerberos)

12. OTP기기는 다음 중 어떤 수단에 해당하는가?

- ① Something You Know
- ② Something You Have
- ③ Something You Are
- ④ Something You Do

13. 2017년에 발표된 OWASP TOP 10의 항목 중 (가)에 해당되는 것은?

- (가)**은(는) 신뢰할 수 없는 데이터가 명령어나 쿼리문의 일부분으로서, 인터프리터로 보내질 때 발생한다. 공격자의 악의적인 데이터는 예기치 않은 명령을 실행하거나 올바른 권한 없이 데이터에 접근하도록 인터프리터를 속일 수 있다.

- ① Broken Access Control
- ② Broken Authentication
- ③ Sensitive Data Exposure
- ④ Injection

14. 다음 설명에 따라 진행되는 공격 유형은?

- 공격자는 악의적인 스크립트가 포함된 콘텐츠를 웹 애플리케이션 서버에 업로드한다.
- 해당 콘텐츠는 웹 애플리케이션 서버에 저장된다.
- 희생자는 해당 콘텐츠를 웹 애플리케이션 서버에 요청하여 수신한다.
- 해당 콘텐츠에 포함된 악의적인 스크립트가 희생자의 디바이스에서 실행된다.

- ① Stored XSS
- ② Reflected XSS
- ③ Brute Force
- ④ Buffer Overflow

15. CSRF에 대한 설명으로 옳은 것은?

- ① 취약한 컴포넌트를 악용하여 공격하면 데이터 손실이나 서버 장애 문제가 발생할 수 있는 취약점이다.
- ② 조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리를 이용해 가져올 수 있는 취약점이다.
- ③ 적절히 보호되지 않은 쿠키를 사용하여, 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점이다.
- ④ 로그인한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 전송할 수 있는 취약점이다.

16. 다음에서 설명하는 검사 도구는?

- 어느 한 시점에서 시스템에 존재하는 특정 경로 혹은 모든 파일에 관한 정보를 DB화하여 저장한 후, 수정·삭제·생성된 파일에 관한 정보를 알려주며, 해커들에 의한 파일의 위변조 여부를 판별할 수 있는 기능을 제공해 주는 검사 도구이다.

- ① Tripwire ② Burp Suite
③ Snort ④ NESSUS

17. robots.txt 파일에 대한 설명으로 옳은 것은?

- ① robots.txt 파일은 웹 루트 디렉터리에 위치한다.
- ② User-agent는 접근거부 디렉터리를 나타내는 키워드이다.
- ③ Disallow는 검색 엔진 종류를 나타내는 키워드이다.
- ④ User-agent와 Disallow는 동시에 사용할 수 없다.

18. 다음은 Windows 운영체제가 설치된 시스템에서 SID를 출력한 결과이다. (가), (나)에 대한 설명으로 옳지 않은 것은?

- S-1-5-21-2823624781-484892517-3265479878-500
(가) (나)

- ① (가)는 시스템 부팅 시마다 새롭게 부여되는 시스템 ID이다.
- ② (나)는 RID를 나타내며, 500의 경우 Administrator임을 의미한다.
- ③ (나)는 RID를 나타내며, 501의 경우 Guest임을 의미한다.
- ④ (나)는 RID를 나타내며, 일반 사용자에게는 1,000 이상의 숫자가 부여된다.

19. 디지털 포렌식의 절차에서 사전준비 이후 단계를 순서대로 바르게 나열한 것은?

- (가) 증거 수집
(나) 보관 및 이송
(다) 보고서 작성
(라) 증거 분석 및 조사

- ① (가) → (나) → (다) → (라)
 ② (가) → (나) → (라) → (다)
 ③ (나) → (가) → (다) → (라)
 ④ (나) → (라) → (가) → (다)

20. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

- CVE(Common Vulnerabilities and Exposure)는 공개적으로 알려진 소프트웨어의 보안취약점을 가리키는 고유 표기를 의미한다.
- 취약점명은 CVE- [(가)] - [(나)] 형식으로 구성되어 있다.

- | (가) | (나) |
|--------|----------|
| ① 일련번호 | 소프트웨어 버전 |
| ② 연도 | 소프트웨어 버전 |
| ③ 일련번호 | 연도 |
| ④ 연도 | 일련번호 |