2019년 경찰간부
시스템네트워크보안(주관식)

-2019년 10월 5일 시행

☑ 만든이 : 지안에듀 조현준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ 저서

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ 무료 동영상 안내

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

1. ○△× 19.경간부

【문 1】 다음은 버퍼 오버플로우 공격 기법(Buffer Overflow Attack)에 대한 문항이다. 아래 물음에 답하시오. (50점)

(1) 힙(Heap) 버퍼 오버플로우와 스택(Stack) 버퍼 오버플로우 기법에 대해 기술하시오. (20점)

◦ 스택 버퍼 오버플로우 공격은 보통 SetUID(Set User ID)가 설정된 루트 권한의 프로그램을 공격대상으로 한다. 스택에 정해진 버퍼보다 큰 공격 코드를 삽입하여 반환주소를 변경함으로써 임의의 공격 코드를 루트 권한으로 실행하도록 하는 방법이다.

◦ 힙에 요청되는 메모리는 레코드의 연결리스트와 같은 동적 데이터 구조를 위해 사용된다. 만약 이런 레코드가 오버플로우에 취약한 버퍼를 가지고 있다면 연속된 메모리가 손상될 수 있다. 스택과는 다르게 실행 제어를 쉽게 이동시킬 수 있는 반환 주소는 없다. 그러나 할당된 공간이 함수에 대한 포인터를 포함하고 있다면 공격자는 이 주소를 변경하여 겹쳐 쓴 버퍼에 있는 셸코드를 가리키도록 할 수 있다.

(2) 다음은 버퍼 오버플로우를 일으킬 수 있는 취약한 C언어 함수이다. 해당 함수를 보완한 안전한 함수의 이름과 안전한 이유에 대해 기술하시오. (15점)

보기

```
strcpy(char *dst, const char *src)
```

◦ 안전한 함수: strncpy(char *dest, const char *src, size_t len) → src 문자열의 len 만큼을 dest 버퍼에 저장한다.

◦ 안전한 이유: 버퍼 오버플로우에 취약한 함수와 그렇지 않은 함수가 있는데, 프로그래머가 취약한 특정 함수를 사용해야 공격이 가능하다. 그러므로 취약한 함수를 사용하지 않는 프로그래머만 있으면 버퍼 오버플로우 공격이 훨씬 어려워진다.

(3) 다음의 스택 버퍼 오버플로우 대응 기술에 대해 기술하시오.(15점)

① 스택 가드(Stack Guard)

스택 오버플로우 공격에 대해 프로그램을 보호하는 효과적인 방법 중 하나는 함수의 진입(entry)과 종료(exit) 코드를 조사하고 함수의 스택 프레임에 대해 손상이 있는지를 검사하는 것이다. 어떤 변경이 발견된다면 공격을 계속 허용하는 대신 프로그램을 종료시킨다. Stack Guard는 가장 잘 알려진 보호 메커니즘 중 하나이다.

② 스택 쉴드(Stack Shield)

함수 시작 시 복귀 주소(Return Address)를 Global RET라는 특수 스택에 저장해 두었다가 함수 종료 시 저장된 값과 스택의 RET값을 비교해 다를 경우 오버플로우로 가정하여 프로그램 실행을 중단시키는 기술을 말한다.

③ 주소 공간의 임의 추출(ASLR)

공격을 막는 다른 실행 시간 기법으로는 프로세스 주소 공간에 있는 중요 데이터 구조의 위치를 조작하는 것이 있다. 공격자는 셸코드로 제어를 넘기기 위해 공격에 사용할 적당한 반환주소를 결정하는데 예측된 주소를 사용한다. 이 예측을 어렵게 만드는 한 가지 기법은 각 프로세스 안의 스택이 임의의 다른 곳에 위치하도록 변경하는 것이다.

2. ○△× 19.경간부

【문 2】 포트 스캐닝(Port Scanning)은 어떤 포트가 열려 있는지 확인하는 것으로 침입 전 취약점을 분석하기 위한 사전 작업 중 하나이다. 아래 물음에 답하시오. (20점)

(1) TCP Connect(Open) 스캔에 대해 약술하시오. (6점)

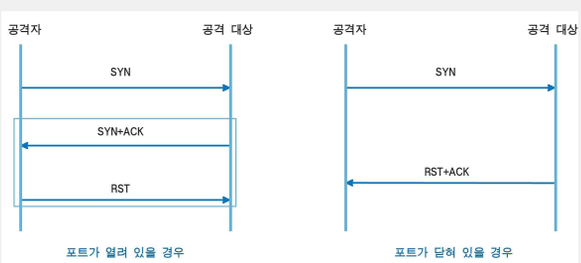
◦ TCP Full Open 스캔은 포트가 열려 있는 경우 대상시스템으로부터 SYN/ACK 패킷을 수신하면 그에 대한 ACK 패킷을 전송함으로써 연결을 완료하는 방식이다.

◦ 포트가 닫혀 있을 경우에는 대상 시스템이 연결 요청을 받아들이지 못하므로 RST/ACK 패킷을 전송한다.

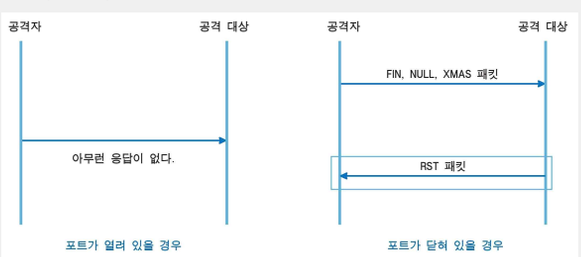
◦ TCP Full Open 기법은 스캔하고자 하는 포트에 접속을 시도해 완전한 TCP 연결을 맺어 신뢰성 있는 결과를 얻을 수 있으나, 속도가 느리고 로그를 남기므로 탐지가 가능하다는 단점이 있다.

(2) TCP FIN·NULL·Xmas 스캔을 각각 설명하고, SYN 스캔(Half-Open Scan)과의 응답 결과에 대한 차이점을 약술하시오. (8점)

◦ TCP Half Open 스캔



◦ FIN, NULL, XMAS 스캔



(3) Decoy 스캔에 대해 약술하시오. (6점)

decoy는 유인한다는 의미로 스캔을 당하는 대상 호스트에서 스캐너 주소를 식별하기 어렵도록 실제 스캐너 주소 외에 다양한 위조된 주소로 스캔하는 방식을 말한다. 다양한 IP로 스캐너 주소를 위조하여 관리자가 스캔을 누가 하는지 알아채기 어렵도록 한다.

3. ○△× 19.경간부

【문 3】 스위치 환경에서 가능한 스니핑 공격 기법에 대해 약술하시오. (30점)

◦ 스위치 재밍(Switch Jamming)은 스위치의 MAC Address Table의 버퍼를 오버플로우시켜서 스위치가 허브처럼 동작하게 강제적으로 만드는 기법을 말한다. 스위치는 Fail Open정책, 즉 실패 시에 모두 허용해주는 정책을 따르는 장비이므로 문제가 발생하면 Hub처럼 연결된 모든 노드에게 패킷을 전송한다. MAC Address Table을 채우기 위해 MAC주소를 계속 변경하면서 ARP Reply 패킷을 지속적으로 전송하는 방식으로 공격한다.

◦ ARP 스푸핑(Spoofing): 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply패킷을 만들어 희생자에게 지속적으로 전송하면 희생자의 ARP Cache에 특정 호스트의 MAC 정보가 공격자의 MAC 정보로 변경이 된다. 이를 통해서 희생자로부터 특정 호스트로 나가는 패킷을 공격자가 스니핑하는 기법이다.

◦ ARP 리다이렉트(Redirect): 공격자가 자신이 라우터인 것처럼 MAC주소를 위조하여 ARP Reply패킷을 해당 네트워크에 broadcast한다. 이를 통해 해당 로컬 네트워크의 모든 호스트와 라우터 사이의 트래픽을 스니핑하고, IP Forward기능을 통해 사용자가 눈치 채지 못하도록 하는 기법이다.

◦ ICMP 리다이렉트는 3계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.

◦ 스위치의 SPAN/Port Mirroring 기능은 스위치를 통과하는 모든 트래픽을 볼 수 있는 기능으로 특정 포트에 분석 장비를 접속하고 다른 포트의 트래픽을 분석 장비로 자동 복사해주는 기술이다. 관리적인 목적으로 사용하지만 공격자가 물리적으로 해당 포트에 접근할 수 있다면 손쉽게 패킷을 스니핑할 수 있다.

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조