2016년 08회
239. 다음 설명에 해당되는 공격 유형은?

▪ 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다. ▪ 버그를 갖고 있는 System Program과 침입자의 Exploit Program이 거의 같은 시간대에 실행되어 System Program이 갖는 권한으로 Exploit Program이 실행되는 경우를 말한다.

① Stack Based Buffer Overflow
② Format String
③ Race Condition
④ Synchronization

정답 3

취약점 개요 p.605

2017년 09회
240. ㉠, ㉡에 해당하는 보안도구로 적절한 것은?

ㄱ. SATAN, SAINT, COPS, Nessus, Nmap 등의 보안도구들을 통칭하는 용어 ㄴ. 유닉스에서 실시간 트래픽 분석과 IP 네트워크상에서 패킷로깅이 가능한 대표적인 네트워크 침입탐지 시스템으로 공개용 소프트웨어이다.

① ㉠ 취약점 점검도구, ㉡ Snort
② ㉠ 도칭 도구, ㉡ SNMP
③ ㉠ 침입 탐지 도구, ㉡ SNMP
④ ㉠ 무결성 검증 도구, ㉡ Snort

정답 1

2018년 11회
241. 취약점 점검용으로 사용되는 도구가 아닌 것은?
① SATAN ② Nessus
③ Sandbox ④ ISS

정답 3

Sandbox는 응용프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 돌립되어 실행되는 형태를 말한다.

2019년 14회

242. 포트 스케닝 도구로 해커가 설치한 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 프로그램으로 옳은 것은?

① ps ② nmap

③ nslookup ④ traceroute

정답 2

nmap: 네트워크 취약점 도구로 백도어와 연관된 포트가 열려있는지 확인할 수 있다.

2015년 05회

243. 다음은 스캔 도구로 유명한 Nmap의 스캔 타입을 설명한 내용이다. 보기에서 설명하는 스캔 타입은 무엇인가?

Half-open 스캐닝을 위해 사용하는 옵션은? TCP SYN 을 확인하는 옵션

① -sX ② -sS

③ -sU ④ -sP

정답 2

스캔	옵션	설명
TCP SYN 스텔스	-sS	프로토콜(TCP) 포트를 스캔하는데 가장 빠른 방법으로 지금까지 단연 인기 있는 스캔 방법이다. 이 스캔은 연결 스캔보다 더 비밀스러우며 모든 기능적인 TCP 스택에 대해 잘 작동한다.
TCP 연결	-sT	연결 스캔은 대부분의 다른 방법처럼 로우 패킷에 의존하기 보다는 장치를 스캔하는데 같은 이름의 시스템 콜을 사용한다.
UDP	-sU	UDP포트 스캔이다.
TCP ACK	-sA	ack스캔은 보통 방화벽 규칙 세트를 정밀하게 표시하기 위해 사용한다.
TCP FTP 바운스	-b	tcp FTP 바운스 스캔 종류는 FTP서버를 속여 프록시로 포트 스캔을 수행하게 한다.

표 324 Nmap포트스캔 옵션

2013년 02회

244. 익명의 FTP 서버를 통해 바운스공격시 사용하는 nmap 스캔타입은 무엇인가?

① -b ② -sW

③ -sU ④ -sA

정답 1

취약점 점검도구

도구명	설명
Nessus	시스템 취약점 점검 툴
Tcpdump	네트워크 모니터링 및 데이터 획득
pwdump	**윈도우에서 패스워드를 덤프할 수 있는 도구이다.**
Snort	**공격 탐지 패킷 스니퍼/로그(sniffer/logger)**
Saint	**보안 점검 툴 악용 시 해킹의 도구가 될 수 있음**
Etereal	네트워크 트래픽 분석기
Internet Security Scanner	네트워크 보안 스캐너
DSniff	패스워드 그리고 다른 정보를 위한 스니퍼
Tripwire	**파일 및 디렉터리 무결성 점검**
Cybercop	스캐너(상용)
Hping2	방화벽 규칙 테스터,포트 스캐닝
SARA	보안 분석 툴
Sniffit	**TCP/UDP/ICMP 패킷을 스니퍼**
SATAN	**취약점 분석**
IPFilter	방화벽 환경에서 사용하기에 적절한 TCP/IP 패킷 필터
iptables/netfilter/ipchains/ipfwadm	커널 2.4.x을 위한 IP 패킷 필터
Firewalk	IP 패킷 응답 분석
Strobe	TCP port scanner
L0pht Crack	**NT 패스워드 검사**
John the Ripper	**패스워드 크래킹 툴** 해시값을 패스워드가 저장된 shadow파일에서 찾아 크랙하는 방식을 취한다.
Hunt	packet sniffer and connection intrusion
OpenSSH / SSH	리모트 시스템에 로긴, 명령어 수행
tcp wrappers	telnet, ftp, rsh, rlogin, finger 등등으로 들어오는 client host 이름 기록
NTop	자신의 네트워크 상의 시스템 용도 요약
NAT	목표 시스템에 의해 제공되는 NETBIOS 파일 공유 서비스 확인
scanlogd	포트스캔 탐지
Sam Spade	IP주소 및 스패머 추적
NFR	침입탐지 시스템을 만들기 위한 스니핑 어플리케이션
logcheck	관리자에게 로그 파일 중 이상한 점 메일을 보냄
Perl	강력한 스크립팅 언어
Ngrep	네트워크 트래픽 grep
Cheops	로컬 및 리모트 네트워크 맵핑, OS형태 알려줌
Vetescan	취약점 스캐너
Retina	보안 스캐너
Libnet	쓰고 통제할 수 있는 low-level네트워크 패킷 프레임 제공
Crack/Libcrack	패스워드 크랙
Cerberus Internet Scanner	보안 스캐너
Swatch	로그파일에 쓰여지는 메시지 모니터

Nemesis	간단한 쉘스크립트로 패킷 흐름을 스크립팅
LSOF	유닉스 전문 진단 툴
Lids	침입 탐지 및 방어
IPTraf	IP LAN 모니터
IPLog	TCP/IP 트래픽 로그
Fragrouter	NIDS의 정확성 테스트
Queso	OS 탐지
GPG/PGP	암호화 프로그램
syslog	로깅 메시지 프로그램 표준으로 다양한 프로그램이 생성하는 메시지들을 저장하고 이들 메시지를 이용해서 다양분석 등이 가능하도록 로그 메시지들을 제공한다.
AWstats	웹로그 분석을 수행하는 프로그램으로 홈페이지에 접속한 사용자에 대한 분석이 가능하다.
Webablizer	로그 분석하기 위한 툴로 홈페이지에 접속한 사용자에 대한 분석이 가능하다.

표 326 다양한 취약점 점검 도구

라) 취약점 점검 도구

(1) SAINT(Security Administrator's Integrated Network Tool)

① **SAINT는 취약점 점검도구이다**.

② SAINT는 기존의 네트워크 보안취약점진단도구인 SATAN과 프로그램구조가 매우 흡사하며 GUI 등 사용자 인터페이스와 결과 리포트도 HTML 문서로 제공하는 등 거의 유사하다.

(2) Nmap(Network Mapper)

① **네트워크 취약점 점검 도구**이다.

② **네트워크 보안을 위한 유틸리티로 대규모 네트워크를 고속으로 스캔하는 도구이다**.

③ Nmap은 포트스캐닝 도구로 해커가 설치한 백도어와 연관된 포트가 열려있는지 확인할 수 있다.

④ **네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로, TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용된다**.

(3) SATAN(Security Analysis Tool for Auditing Networks)

① **네트워크상에서 문제점이 발생할 경우 문제점에 대한 원인 정보 제공 등과 함께 해결책을 제시하는 보안 스캐너이다**.

2015년 06회
245. 다음 중 무결성 점검 도구로 그 성격이 다른 것은?
① tripwire ② fcheck
③ md5 ④ nessus

정답 4

- tripwire, fcheck, md5는 무결성 점검 도구이다.
- nessus는 취약성 점검 툴이다.

2013년 01회
246. 다음 중에서 시스템의 취약성 점검을 위하여 사용할 수 있는 도구가 아닌 것은?
① ping ② SATAN
③ SAINT ④ NESSUS

정답 1

2016년 07회
247. 다음 중 취약점 점검과 가장 거리가 먼 보안 도구는?
① SATAN ② COPS
③ Nmap ④ Tripwire

정답 4

- tripwire는 무결성 점검 도구이다.

2015년 05회
248. 다음 중 취약성 점검 도구가 아닌 것은?
① nikto2 ② SARA
③ NESSUS ④ Tripwire

정답 4

- tripwire는 무결성 점검 도구이다.

2014년 04회
249. 다음 중 취약성 점검도구가 아닌 것은 무엇인가?
① NESSUS ② SARA
③ NIKTO2 ④ TRIPWIRE

정답 4

- tripwire는 무결성 점검 도구이다.

2019년 14회

250. 다음 중 인터넷 전자상거래에서 무결성(Integrity) 점검을 위해 쓰이는 해시 함수가 아닌 것은?

① tripwire ② MD5

③ RIPEMD-160 ④ SHA-256

정답	1

Tripwire: 파일의 무결성 점검을 위한 도구로 이를 위해 체크 썸(Check Sum) 값을 이용해 트로이목마 프로그램을 감지하기 가장 알맞은 툴이다.

2016년 08회

251. 다음 중 무결성(Integrity) 점검을 위한 해시 함수가 아닌 것은?

① tripwire ② MD5

③ SHA-256 ④ RIPEMD-160

정답	1

2017년 10회

252. 다음 중 취약점 점검 도구와 가장 거리가 먼 것은?

① SATAN ② Tripwire

③ Nessus ④ OOPS

정답	2

2016년 08회

253. 다음 중 무결성 점검을 위해 사용하는 프로그램은?

① tripwire ② tcpdump

③ hunt ④ dsniff

정답	1

2015년 05회
254. 다음의 취약성 점검 도구 중 NESSUS 도구로 탐지할 수 없는 것은?
① 사용할 때만 열리는 닫힌 포트
② 쿠키값
③ 운영 체제 종류
④ 웹 서버 취약점

정답 2

2016년 08회
255. 다음의 공격도구들이 공통적으로 제공 기능은?

John the Ripper, pwdump, L0phCrack

① Brute Force 공격 ② Web 공격
③ 스니핑 공격 ④ 사회 공학 공격

정답 1

2016년 07회
256. Brute Force Attack 및 Dictionary Attack 등과 가장 거리가 먼 것은?
① John the Ripper ② L0phtcrack
③ Pwdump ④ WinNuke

정답 4

2013년 01회
257. 다음 중에서 snort를 이용하여 탐지할 수 없는 공격은 무엇인가?
① 버퍼 오버플로우(Buffer OverFlow)
② 사전 공격(Dictionary Attack)
③ TCP SYN Flooding
④ IP Filtering

정답 2

2014년 04회
258. 다음 리눅스 iptables에서 chain 형식으로 사용이 옳지 않은 것은?
① INPUT ② FORWORD
③ OUTPUT ④ DROP

정답 4

iptables는 시스템 관리자가 리눅스 커널 방화벽(다른 넷필터 모듈로 구현됨)이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 사용자 공간 응용 프로그램이다.
5개의 미리 정의된 체인들이 존재한다.

- PREROUTING: 패킷들은 라우팅 결정이 만들어지기 전에 이 체인에 들어갈 것이다.
- INPUT : 패킷이 로컬상에서 전달될 경우, 이것은 열린 소켓을 가진 프로세스들과 아무런 상관이 없다; 로컬 전달은 "local-delivery"라우팅 테이블에 의해 제어된다: ip route show table local.
- FORWARD : 라우팅되고 로컬 전달이 아닌 모든 패킷들은 이 체인을 순회한다.
- OUTPUT : 기계 자체에서 보내진 패킷들은 이 체인을 마주칠 것이다.
- POSTROUTING: 라우팅 결정이 만들어졌을 때, 패킷들은 하드웨어에 보내지기 전에 이 체인에 들어온다.

2014년 04회
259. 다음 보기를 보고 올바르게 설명하고 있는 것을 고르시오.

```
# iptables -A INPUT -s 172.10.10.10 -p tcp -j drop
```

① 외부 ip 172.10.10.10 에서 들어오는 패킷을 차단한다.
② 내부 ip 172.10.10.10 에서 나가는 패킷을 차단한다.
③ 외부 ip 172.10.10.10 에서 나가는 패킷을 차단한다.
④ 내부 ip 172.10.10.10 에서 들어오는 패킷을 차단한다.

정답 1

2015년 06회
260. 다음 중 iptables에서 체인 형식으로 사용하지 않는 것은?
① OUTPUT ② INPUT
③ DROP ④ FORWORD

정답 3

2014년 04회

261. 다음 중 IPTABLES에서 새로운 규칙을 출력하는 옵션은?

① -p ② -D

③ -A ④ -L

정답	4

- I chain [룰번호], --insert chain [룰번호] : 체인 정책에 새로운 룰을, 지정한 위치(룰번호)나 맨 뒤에 삽입한다.
- R chain 룰번호, --replace : 체인 정책의 지정 위치(룰번호)에 있는 룰을 교체한다.
- L [chain], --list [chain] : 모든 체인 정책을 보거나, 지정한 체인 정책을 본다.
- F [chain], --flush : 모든 체인 정책을 삭제하거나, 지정한 체인 정책을 삭제한다.
- Z [chain], --zero : 모든 체인 정책을 비우거나, 지정한 체인 정책을 비운다.

2013년 01회

262. 서버 보안을 강화하기 위한 방법으로 서버에 들어오고 나가는 IP 트래픽을 제어할 수 있는 방법은?

① ipchain/iptable

② IP Control/mod_security

③ mod_security/nmap

④ IP Manager/IP Filtering

정답	1

2016년 07회

263. 다음 보기 중 그 성질이 다른 것은?

① SQL Injection

② XSS or GSS(Cross site Scription)

③ Cookie sniffing

④ Whois

정답	4