신뢰 플랫폼 모듈(TPM: Trusted Platform Module) p.511

2014년 04회

50. 윈도우즈 운영체제에서 네트워크상 관리목적으로 기본 공유폴더를 삭제하는 알맞은 명령어는 무엇인가?

① net Share_Dir / delete
② net share Share_Dir /delete
③ net delete
④ net share delete

정답	2

1. net share : 공유 폴더 확인 명령
2. 실행예시

```
C:₩Users₩itwiki>net share

공유 이름    리소스                          설명
-------------------------------------------------------------------------------
C$           C:₩                             기본 공유
D$           D:₩                             기본 공유
IPC$                                         원격 IPC
ADMIN$       C:₩Windows                      원격 관리
명령을 잘 실행했습니다.
```

3. 공유폴더 보안
   - Windows는 관리 목적상 ADMIN$, C$, D$, IPC$ 를 기본적으로 공유하도록 설정되어 있음
   - 필요하지 않다면 보안성 향상을 위해 공유 설정을 꺼 주는 것을 권장
4. Null Session Share 취약점
   - 윈도우가 설치된 서버에 IPC$를 통한 원격접속을 할 때 패스워드를 Null로 설정하여 접속할 수 있는 취약점
   - 공격자가 시스템의 유저명, 공유정보 등을 열람할 수도 있고 일부 레지스트리에 접근할 수 있으며 DoS공격에도 활용 될 수 있음
5. 공유폴더 제거
   - net share 공유폴더명 /delete
   - IPC : 프로세서 간 통신(interprocessor communication)의 약어.

클라이언트 보안: 악성 소프트웨어(악성 코드) p.513

2018년 11회

51. 다음 중 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은

① 부트 바이러스란 플로피디스크나 하드디스크의 부트섹터를 감염시키는 바이러스를 말한다.

② 파일 바이러스는 숙주 없이 독자적으로 자신을 복제해 다른 시스템을 자동으로 감염시켜 자료를 유출, 변조, 삭제하거나 시스템을 파괴한다.

③ 이메일 또는 프로그램 등의 숙주를 통해 전염되어 자료를 변조, 삭제하거나 시스템을 파괴한다.

④ 최근 들어 암호화 기법을 기반으로 구현된 코드를 감염 시마다 변화시킴으로써 특징을 찾기 어렵게 하는 다형성 (Polymorphic) 바이러스로 발전하고 있다.

정답	2

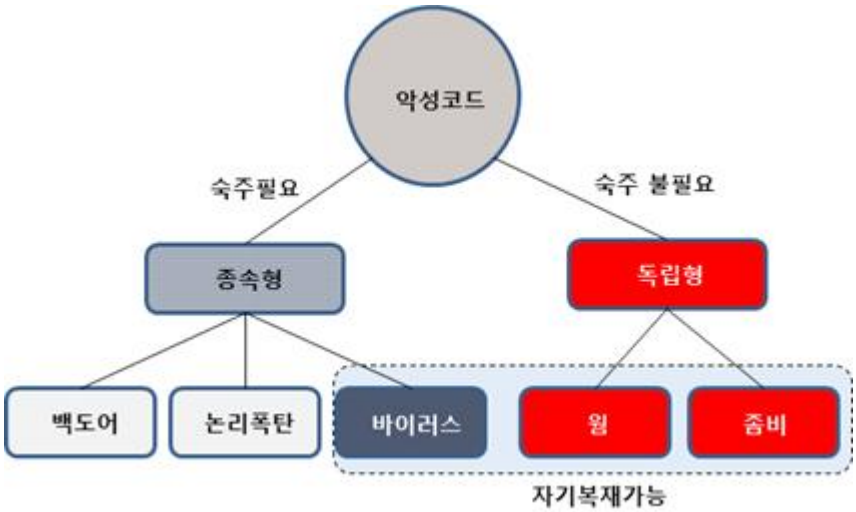

그림 20 악성 소프트웨어(악성 코드)

바이러스 : 숙주필요(종속형), 자기복재 가능

2017년 09회

52. 다음 중 운영체제와 무관하게 매크로 기능이 있는 MS 오피스 제품과 같은 프로그램을 통해 활동하는 컴퓨터 바이러스에 해당하는 것은?

① 매크로(Macro) 바이러스

② 다형성(Polymorphic) 바이러스

③ 은폐형(Stealth) 바이러스

④ 암호형(Encryption) 바이러스

정답	1

2017년 10회

53. Visual Basic 스크립트를 이용한 악성코드에 대한 설명으로 맞는 것은?

① 웹브라우저에서 실행될 경우 스크립트가 브라우저에 내장되므로 파일의 내용을 확인하기 어렵다.

② 독립형으로 개발할 경우 파일 생성에 제한을 받아 웜형 악성코드를 만들지 못한다.

③ 확장자는 VBA다.

④ 이메일에 첨부되어 전파될 수 있다.

정답	4

■ 바이러스, 웜, 트로이 목마 비교

구분	바이러스	웜	트로이 목마
특징	사용자 컴퓨터 내에서 자신 또는 자신의 변형을 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다.**(숙주 필요)**	시스템 및 응용 소프트웨어의 취약점을 악용하거나 전자우편 또는 공유 폴더를 이용하며, 네트워크를 통해서 컴퓨터에서 컴퓨터로 빠르게 전파된다.**(숙주 불필요)**	겉으로 보기에는 유용해 보이지만 정상적인 프로그램 속에 숨어있는 악성 소프트웨어로, 사용자가 프로그램을 실행할 때 동작한다.
복사 및 전염능력	있음	매우 강함	없음
형태	파일이나 부트섹터 등 감염대상 필요	독자적으로 존재	유틸리티로 위장하거나 유틸리티 안에 코드 형태로 삽입
전파 경로	사용자가 감염된 파일을 옮김	네트워크나 전자메일을 통해 스스로 전파	사용자가 내려 받음
주요 증상	해당 컴퓨터의 시스템 및 파일 손상	**시스템에 직접적인 영향은 미치지 않는 악성 프로그램**으로 주로 네트워크 성능 저하를 일으킨다.	PC성능 저하, 좀비 PC, 데이터 유출
방어 방법	백신, 안티바이러스	N-IDS	H-IDS
침해 보안 목표	무결성 침해	가용성 침해	기밀성 침해

표 71 바이러스, 웜, 트로이 목마 비교

트로이목마 p.521

2019년 14회

54. 다음 중 트로이 목마(Trojan)의 일반적인 특징 및 기능으로 옳지 않은 것은?2

① 패스워드 가로채기
② 악성코드 전파
③ 파일 파괴
④ 원격 조정

정답	2

트로이 목마는 정상적인 프로그램으로 가장한 악성 프로그램으로 정보를 빼내기도 하고, 파일을 지우기도 한다. 다만 자기복제 능력은 없다.

2018년 11회

55. 트로이목마의 특징이 아닌 것은?

① 백도어(Back Door)로 사용할 수 있다.
② 자기복제 능력이 있다.
③ 유용한 프로그램에 내장되어 배포될 수 있다.
④ 정보유출이나 자료파괴 같은 피해를 입힐 수 있다.

정답	2

2018년 11회

56. 다음 지문은 무엇을 설명한 것인가?

일반 프로그램에 악의적인 루틴을 추가하여 그 프로그램을 사용할 때 본래의 기능 이외에 악의적인 기능까지 은밀히 수행하도록 하는 공격을 말한다. 예를 들어 사용자 암호를 도출 하기 위해서 합법적인 로그인(login) 프로그램으로 가장하고 정상적인 로그인 순서와 대화를 모방하여 작성될 수 있다.

① 트로이목마(Netbus)
② 매크로 바이러스(Macro virus)
③ 웜(I-Worm/Hybris)
④ 악성 스크립트(mIRC)

정답	1

2016년 07회
57. 다음은 트로이목마의 특징에 대한 설명이다. 성격이 가장 다른 하나는?
① 원격조정 ② 시스템 파일 파괴
③ 자기복제 ④ 데이터 유출

정답	3

2013년 02회
58. 다음 중 트로이 목마에 대한 설명으로 올바르지 않은 것은?
① 악의적으로 제작되었다.
② 유틸리티 프로그램에 내장되어 있다.
③ 백오리피스 같은 프로그램이 대표적인 사례이다.
④ 트로이목마는 자기 복제가 가능하다.

정답	4

2018년 12회
59. 다음은 여러가지 멀웨어에 대한 설명이다. 올바르지 않은 것은?1
① 바이러스와 트로이 목마는 자가 복제되서 스스로 전파되는 특징이 있다.
② 바이러스가 다른 실행프로그램에 기생하는데 반해 웜은 독자적으로 실행된다.
③ 스파이웨어는 사용자의 동의 없이 설치되어 사용자의 행동을 감시하고 개인정보를 유출한다.
④ 애드웨어는 사용자의 동의 기반으로 설치된 경우 멀웨어로 구분할 수 없다.

정답	1

2018년 12회
60. 다음 악성코드에 대한 설명 중 옳지 않은 것은?513
① 루트킷(Rootkit)은 단일 컴퓨터 또는 일련의 컴퓨터 네트워크에 대해 관리자 레벨의 접근을 가능하도록 하는 도구의 집합이다.
② 웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성 프로그램으로 보통 복제 과정을 통해 스스로 전파된다.
④ 트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.

정답	3

트로이 목마(Trojan horse)는 정상적인 프로그램으로 가장한 악성 프로그램이다. 자기복제 능력이 없이 악의적인 작업을 수행하는 악성코드가 숨겨져 있는 정상을 가장한 프로그램이다.

2016년 07회

61. 트로이목마 프로그램으로 사용자의 키보드 입력을 가로채는 목적으로 사용되기 때문에 이 프로그램이 동작하는 컴퓨터에서 입력되는 모든 것이 기록되어 개인정보 등이 도용당하게 되는 해킹기법은 무엇인가?

① 포트스캔 ② 쿠키
③ DoS ④ 키로그

정답 4

크로그 S/W는 트로이목마에 이용되는 프로그램으로 사용자의 키보드 입력을 가로채는 목적으로 사용되기 때문에 이 프로그램이 동작하는 컴퓨터에서 입력되는 모든 것이 기록되어 개인정보 등이 도용당하게 되는 해킹기법이다.

2013년 01회

62. 다음에서 설명하는 공격용 소프트웨어는 무엇인가?

. 안티바이러스 프로그램에 의해 탐지된다. . 특정 문자열을 타이핑한 후 파일의 내용에서 타이핑한 문자열이 검색된다. . 지정된 시간에 로그파일을 설정된 공격자 메일로 자동 전송기능을 포함한다. . 소프트웨어로 winhawk가 있다.

① Root Kit ② Key Logger software
③ Port Scanning ④ Nessassin

정답 2

2018년 11회

63. 다음 중 악성코드의 치료 방법이 다른 것은?(참고용)

① 바이러스 ② 웜
③ 트로이목마 ④ 스파이웨어

정답 4

2017년 10회

64. 논리폭탄에 대한 특징을 설명하고 있는 것은?

① 프로그래머나 시스템 관리자가 그들만이 사용할 수 있도록 소프트웨어에 보안 hole을 만들어 놓는다.
② 컴파일러 개발자가 컴파일러 안에 악성코드를 삽입하여 유포함으로써, 소프트웨어의 소스코드에서는 악성코드를 찾을 수 없도록 하였다.
③ 프로그램 환경변수들이 사전 정의된 값과 일치되면 악성행위를 수행 한다.
④ 자기 복제기능을 갖고 있다.

정답 3

논리폭탄 : 특정한 시간에 적국의 컴퓨터 파일을 교란시키도록 프로그램 된 일종의 시한폭탄과 같은 컴퓨터 바이러스라고 할 수 있다.

2017년 09회
65. 특정 조건이 만족될 때까지 잠복하고 있다가 조건이 만족되면 트리거 되어 해커가 원하는 동작을 실행하는 공격방법은?
① 트로이 목마 ② 키로거
③ 논리 폭탄 ④ 백도어 (Backdoor)

정답 3

2013년 02회
66. 다음 중 백도어나 바이러스, 웜에 감염되면 주로 사용하는 프로세스는 무엇인가?
① explore.exe ② winupdate.exe
③ svchost.exe ④ hosts

정답 3

svchost.exe : 윈도우 서비스를 담당하고 있는 시스템 프로세스이다. DLL에 의해 실행되는 프로세스의 기본 프로세스이며 한 시스템에 여러 개의 svchost 프로세스를 볼 수 있다.

루트킷 p.526

2015년 06회
67. 다음 중 루트킷에 대한 설명으로 올바르지 못한 것은?
① 로그 파일을 수정한다.
② 루트킷은 자기 복제가 가능해 다른 PC에도 설치된다.
③ 시스템 흔적을 제거한다.
④ 기존 시스템 도구들을 수정한다.

정답 2

루트킷은 시스템 침입 후의 공격을 도와주는 프로그램의 집합으로 해커들의 도구모음이다.

2015년 06회
68. 다음 중 안티 루트킷의 주요 기능이 아닌 것은?
① 숨김 파일 찾기 ② 수정된 레지스트리 찾기
③ 프로세스 보호 해제 탐지 ④ 로그 파일 흔적 제거

정답 4

안티 루트킷의 주요 기능은 숨겨진 파일 찾기, 수정된 레지스트리 찾기, 보호 해제된 프로세스 탐지 이다.

2015년 05회
69. 다음 중 루트킷에 대한 특징으로 올바르지 못한 것은?
① 트래픽이나 키스트로크 감시 ② 커널 패치
③ 로그 파일 수정 ④ 시스템 흔적 제거

정답 2

인터넷 활용 보안 쿠키 p.534

2017년 10회

70. 웹 브라우저가 웹서버에게 쿠키 값을 전송할 때 사용하는 HTTP 헤더는?

① Connection ② Proagrma

③ Set-cookie : ④ Cookie :

정답	4

2014년 04회

71. 다음 중 인터넷 익스플로러 브라우저의 보안에 대한 설명으로 올바르지 못한 것은?

① 임시 인터넷파일 저장위치를 변경 할 수 없다.

② 임시 인터넷 파일 폴더에 있는 쿠키를 삭제할 수 있다.

③ 고급 탭에서 HTTP1.1 사용을 설정 할 수 있다.

④ 인터넷 영역에 적용할 보안 수준을 설저알 수 있다.

정답	1

2017년 10회

72. 인터넷 익스플로러에서는 보안 설정을 지정할 웹 콘텐츠 영역을 지정할 수 있다. 다음 중 지정할 수 없는 영역은 어느 것인가?

① 로컬 인트라넷

② 신뢰할 수 있는 사이트

③ 보안 등급 지정 가능한 사이트

④ 제한된 사이트

정답	3