

액티브X, 자바스크립트 p.538

2017년 10회

73. 인터넷 브라우저 공격에 대한 대응방법으로 옳지 않은 것은?

- ① Active X는 "사용함"으로 설정한다.
- ② 백신프로그램을 설치하여 사용한다.
- ③ 신뢰할 수 없는 사이트의 접속을 피한다.
- ④ 브라우저에 최신 버전의 보안패치를 설치한다.

정답 1

2018년 12회

74. 다음 지문에서 설명하고 있는 것은 무엇인가?

최근에 은행, 게임, 음악 등 많은 웹 사이트에서 사용 중인 이것에서 다양한 취약점이 발견되어 사용자의 주의가 요망되고 있다. 이것은 자바 애플릿과는 달리 사용자 PC의 파일, 레지스트리 등 시스템 자원에 접근이 가능하고 공격자가 웹 인터페이스를 통해 언제든지 호출 가능한 취약한 구조로 설계된 경우가 적지 않으며, 이것에서 발생하는 취약점을 이용한 공격은 애드웨어 등에서 널리 사용되고 있다.

- ① 자바스크립트(Javascript)
- ② 액티브엑스(ActiveX)
- ③ 프락시(Proxy)
- ④ 쿠키(Cookie)

정답 2

액티브엑스(ActiveX)는 마이크로소프트 윈도우(Microsoft Windows) 환경에서 응용 프로그램이나 웹 브라우저가 인터넷을 통해 추가 기능을 다운로드 및 실행할 수 있도록 지원하는 소프트웨어 프레임워크이다.

2019년 14회

75. 윈도우에서 관리 목적상 기본적으로 공유되는 폴더 중에서 Null Session Share 취약점을 갖는 것은?

- ① C\$
- ② G\$
- ③ IPC\$
- ④ ADMIN\$

정답 3

Null Session Share 취약점은 윈도우가 설치된 서버에 IPC\$를 통한 원격접속을 할 때 패스워드를 Null로 설정하여 접속할 수 있는 취약점을 말한다.

2017년 09회

76. 다음 보기의 보안 지침 중 옳은 내용을 모두 고른 것은?

- ㄱ. Windows는 관리 특성상 ADMIN\$, C\$, D\$, IPC\$ 등을 기본적으로 공유한다.
- ㄴ. IPC\$ 및 null Seession Share는 제거하는 편이 안전하다.
- ㄷ. IPC\$는 Windows Server 초기 버전에서 해킹된 사례가 있다.
- ㄹ. 숨김 공유를 설정해 놓으면 침입자의 위협을 막을 수 있다.

- ① (ㄱ), (ㄷ) ② (ㄱ), (ㄹ)
- ③ (ㄱ), (ㄹ) ④ (ㄷ), (ㄹ)

정답 1

Windows는 관리 목적상 ADMIN\$, C\$, D\$, IPC\$ 를 기본적으로 공유하도록 설정되어 있음
필요하지 않다면 보안성 향상을 위해 공유 설정을 꺼 주는 것을 권장

윈도우 서버 보안 p.542

2019년 14회

77. 윈도 사용자 권한 통제 방법으로 낮은 권한을 가진 사용자가 관리자 권한을 쓰려고 하면 경고창과 함께 관리자 계정 인증을 요구한다. 이러한 매커니즘을 무엇이라고 하는가?

- ① Privileged Account Management
- ② User Account Control
- ③ User Access Control
- ④ Privileged Access Management

정답 2

UAC(사용자 계정 컨트롤)는 관리자 수준 권한을 필요로 하는 PC 의 변경을 수행하기 전에
사용자에게 알려 주는 기능으로, 유해한 프로그램이 컴퓨터를 변경하는 것을 방지할 수 있다

NTFS p.543

2018년 12회

78. 디스크 공간 할당의 논리적 단위는?

- ① Volume ② Page
- ③ Cluster ④ Stream

정답 3

클러스터(cluster)는 운영 체제에 의해 할당된 장소의 기본적인 단위이다.

2017년 09회

79. 디스크 공간 할당의 논리적 단위는?

- ① Volume ② Page
- ③ Cluster ④ Stream

정답 3

2018년 12회

80. 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?

- ① MFT(Master File Table)
- ② FAT(File Allocation Table)
- ③ \$Attr Def
- ④ \$LogFile

정답 1

MFT(master file table): 모든 파일과 디렉터리에 대한 파일 이름, 크기, 생성 시간 등 파일에 대한 데이터 외의 모든 정보가 저장된다.

2017년 10회

81. 윈도우 NTFS에서 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것은?

- ① MFT(Master File Table)
- ② FAT(File Allocation Table)
- ③ \$AttrDef
- ④ \$Logfile

정답 1

2018년 12회

82. 다음 파일시스템(FAT, NTFS)에 대한 설명 중 옳지 않은 것은?

- ① FAT 뒤의 숫자는 표현 가능한 최대 클러스터 개수와 관련되어 있다.
- ② NTFS 파일시스템은 대용량 볼륨, 보안 및 암호화를 지원한다.
- ③ NTFS 파일시스템은 타 운영체제 호환이 용이하다.
- ④ 저용량 볼륨에서는 FAT가 NTFS보다 속도가 빠르다.

정답 3

NTFS의 단점은 다른 OS와 호환이 불가능하다는 것이다.

2014년 04회

83. 다음 중 윈도우 NTFS 파일 시스템에 대한 설명으로 옳바르지 않는것은?

- ① NTFS 구조는 크게 VBR영역, MFT영역, 데이터영역으로 나눈다.
- ② 이론적인 최대 NTFS 파일 크기는 16EB이다.
- ③ 실제 최대 NTFS파일 크기는 16TB이다.
- ④ 기본 NTFS보안을 변경하면 사용자마다 각기 다른 NTFS보안을 설정할 수 있다.

정답 4

2013년 01회

84. 윈도우의 NTFS 파일시스템 설명으로 옳지 않은 것은?

- ① NTFS의 보안설정은 everyone 그룹에 대하여 모든 권한은 '불가'이다.
- ② net share 폴더에 의해서 공유 폴더를 확인할 수 있다.
- ③ 윈도우 파일시스템에는 FAT16, FAT32, NTFS가 존재하며, NTFS는 윈도우 NT, 윈도우 2000, 윈도우 XP에서 사용된다.
- ④ 윈도우에서는 manager에게 작업을 분담시키고 하드웨어를 제어하는 것은 Object Manager이다.

정답 1

Everone 그룹에 대해 모든 권한 허용

2017년 10회

85. 다음 중 윈도우 시스템의 NTFS 파일시스템에 대한 설명으로 가장 거리가 먼 것은?

- ① NTFS 3.0 버전에서 지원하는 파일 암호화 기법을 NES라고 한다.
- ② NTFS 보안에서는 파일 단위까지 보안을 적용시킬 수 있다.
- ③ 개별 사용자가 그룹 A와 그룹B에 속해 있을 경우에 특정 파일이나 디렉터리에 대한 접근 권한을 그룹 A와 그룹 B의 것 모두 가진다.
- ④ NTFS 접근권한 중 "쓰기" 권한은 해당 디렉터리의 서브디렉터리와 파일을 생성할 수 있다.

정답 1

EFS(Encrypting File System) : 마이크로소프트 윈도우의 NTFS 버전 3.0에서 추가된 파일 시스템 단계 암호화를 하는 기능

2017년 10회

86. 다음 중 NTFS에서 Sector_per_cluster로 정할 수 없는 것은?

- ① 1 ② 6
- ③ 8 ④ 16

정답 2

한 개 클러스터를 구성하는 섹터 수로 2의 제곱수만 가능하다.
즉 2의 배수가 아닌거 고르면 된다.

2014년 03회

87. NTFS에서 Sector_per_cluster로 정할 수 없는 것은 무엇인가?

- ① 1 ② 6
- ③ 8 ④ 16

정답 2

2018년 12회

88. 워너크라이 랜섬웨어와 페트야 랜섬웨어의 차이점을 바르게 설명한 것은?(참고용)

- ① 워너크라이 랜섬웨어에 네트워크 웜 기능이 추가되었다.
- ② MFT(Master File Table) 영역 암호화가 추가되었다.
- ③ 워너크라이 랜섬웨어와 달리 SMB 취약점을 기반으로 한다.
- ④ MBR(Master Boot Record) 영역을 감염시켜서 부팅을 불가능하게 만든다.

정답 4

2017년 09회

89. 최근 APT공격이 지속적으로 발생하고 있다. 다음 사례에서 공통된 내용은 무엇인가?

- 2009년 7.7 디도스
- 2011년 3.4 디도스
- 2013년 3.20 사이버테러

- ① DBMS 파괴 ② Ddos 공격
③ 홈페이지 변조 ④ 마스터부트레코더(MBR) 파괴

정답 4

2015년 05회

90. 다음 중 7.7 DDoS 공격과 3.20 DDoS 공격의 공통점은 무엇인가?

- ① 대역폭 과부하 ② 리소스 고갈
③ MBR 파괴 ④ 금융 정보 유출

정답 3

악성코드 종류	설명 및 특성	대표
바이러스 (Virus)	<ul style="list-style-type: none"> ▪ 다른 독립적 프로그램의 코드 내에 스스로를 주입한 다음, 그 프로그램이 악성 행동을 하고 스스로 확산되도록 강제하는 컴퓨터 코드 	부트(Boot) 바이러스, 파일(File) 바이러스, 매크로 바이러스, 모바일 바이러스
웜(Worm)	<ul style="list-style-type: none"> ▪ 네트워크 등의 연결을 통하여 자신의 복제품을 전파 ▪ 독립적으로 실행됨 	아이러브유, SQL 슬래머(SQL Slammer), MS 블래스터 (MS Blaster)
스파이웨어 (Spyware)	<ul style="list-style-type: none"> ▪ 사용자가 컴퓨터에서 보내고 받는 데이터를 염탐하며 그 목적은 대체로 이 정보를 제 3자에게 보냄 ▪ 일반적으로 제거가 가장 쉬움 	
트로이목마 (Trojans)	<ul style="list-style-type: none"> ▪ 일반 프로그램에 악의적인 루틴을 추가하여 그 프로그램을 사용할 때 본래의 기능 이외에 악의적인 기능까지 은밀히 수행하도록 하는 공격 ▪ 도어(Back Door)로 사용할 수 있음 ▪ 유용한 프로그램에 내장되어 배포될 수 있음 ▪ 정보유출이나 자료파괴 같은 피해를 입힐 수 있음 ▪ 자기복제 능력이 없음 	드롭퍼, 다운로드, 패스워드 스틸러, 프록시, 클리커, 스파이, 익스플로잇
루트킷 (Rootkits)	<ul style="list-style-type: none"> ▪ 단일 컴퓨터 또는 일련의 컴퓨터 네트워크에 대해 관리자 레벨의 접근을 가능하도록 하는 도구의 집합 ▪ 로그 파일을 수정 ▪ 시스템 흔적을 제거 ▪ 기존 시스템 도구들을 수정 	유저 모드 루트킷, 커널 모드 루트킷, 그에 속하지 않는 루트킷(윈도우가 구동되기 전에 동작하는 루트킷)
트랩도어 (Trapdoor)	<ul style="list-style-type: none"> ▪ 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로 	
랜섬웨어	<ul style="list-style-type: none"> ▪ 컴퓨터 시스템에 저장된 사용자 문서 파일을 암호화하거나 컴퓨터 시스템을 잠그고 돈을 요구하는 악성 프로그램으로 전자메일이나 웹사이트 등 다양한 경로를 통해 감염 	크립토월, 크립토락커, CoinVault
논리폭탄 (Logic bomb)	<ul style="list-style-type: none"> ▪ 특정 조건이 만족되면 특정 형태의 공격을 하는 기법 	

윈도우 계정 power user p.546

2018년 12회

91. 다음은 윈도우 사용자 유형에 대한 설명이다. 가장 적절하지 않은 것은?

- ① Administrator : 모든 권한을 가진다.
- ② Power User : 일반 유저지만 관리자의 권한을 가진다.
- ③ Guest: 임시 사용자 계정으로 제한된 권한을 가진다.
- ④ Backup Operator: 백업을 위해 모든 디렉토리에 접근 가능한 권한을 가진다.

정답 2

그룹이름	설명
Administrators	<ul style="list-style-type: none"> 도메인 자원이나 로컬 컴퓨터에 대한 모든 권한이 있다.
Power Users	<ul style="list-style-type: none"> Administrators 그룹이 가진 권한을 대부분 가지나, 로컬 컴퓨터에서만 관리할 능력을 가지고 있다. 시스템에 대한 전체 권한은 없지만 시스템 관리를 할 수 있는 권한이 부여된 계정이다. 컴퓨터에서 로컬 사용자 계정을 생성하고 수정할 수 있는 권한을 갖고 있으며 자원을 공유하거나 멈출 수 있다.
Users	<ul style="list-style-type: none"> 도메인과 로컬 컴퓨터를 일반적으로 사용하는 그룹으로 개개인에 할당된 사용자 환경을 직접 만들 수 있지만, 설정할 수 있는 항목에는 제한이 있다. 시스템 서비스의 시작 및 종료 권한이 없으며, 디렉터리 공유 설정을 할 수 없다.
Gusts	<ul style="list-style-type: none"> 관리자에 의해 허락된 자원과 권한만을 사용하는 도메인 사용권한이 제한된 그룹이다. 시스템 설정 변경 권한이 없다.
Backup Operations	<ul style="list-style-type: none"> Windows 시스템 백업을 위해서 모든 시스템의 파일과 디렉터리에 접근할 수 있다.

2019년 14회

92. 윈도우에서 사용자 계정을 추가하면 일반 사용자 그룹인 User 그룹에 자동 포함된다.

이 User 그룹의 권한에 대한 설명으로 옳지 않은 것을 고르시오.547

- ① User는 워크스테이션을 종료할 수 있고 서버에도 종료 명령을 내릴 수 있다.
- ② User가 로컬 그룹을 만들수는 있지만 자신이 만든 로컬 그룹만 관리한다.
- ③ 관리자가 설치하거나 배포한 인증된 Windows 프로그램을 실행할 수 있다.
- ④ User 그룹의 구성원은 자신의 모든 데이터파일 및 레지스트리에서 자신의 부분을 완전히 제어할 수 있다.

정답 1

Users의 권한은 도메인과 로컬 컴퓨터를 일반적으로 사용하는 그룹으로 개개인에 할당된 사용자 환경을 직접 만들 수 있지만, 설정할 수 있는 항목에는 제한이 있다.

또한 시스템 서비스의 시작 및 종료 권한이 없으며, 디렉터리 공유 설정을 할 수 없다.