MISCCCCCCCCCC

by EverTokki (0415cbl@naver.com)
http://evertokki.tistory.com

들어가며) 서론

<바탕사진 출처: http://goo.gl/uFUDC9>

MISC는 '기타'로 분류되는 항목으로써, 많은 대회에 출제되지만 우리의 실력자분들은 MISC는 거들떠보지도 않고 자신의 분야로 직행하는것을 자주 목격하곤 합니다. 하지만, 요즘 MISC문제들도 꽤나 점수에 많은 공헌을 하고 있으니 한번쯤은 이 문서를 읽어보시는것도 나쁘지 않을것 같습니다. 해당 문서는 그 MISC문제들을 각각 분류해놓음으로써 각각의 문제에 대한 풀이 방법을 제공하고 있습니다. 이 분류들 사이의 선이 흐릿해서 가끔은 카테고리가 다름에도 같은 풀이방법을 사용해야 할 수도 있지만, 그래도 MISC는 MISC입니다. 이 문서로 인해 MISC에 더 많은 관심을 가지실 수 있기를 바랍니다 :)

-MISC는 가끔 특별한 분류가 없는 진짜 문제들일수도 있으니, 이 문서에 있는 모든것이 정확하다고 할 수는 없습니다. 이 문서는 Bonus형(쉬어가는) MISC에 대해 작성한 문서일 뿐입니다.

목차

BONUS 문제

-BONUS문제들은 MISC나 TRIVIA보다도 쉬운 문제입니다. Bonus, 말그대로 잠시 멘붕을 식혀주기 위한 보너스 문제인 것이죠. 대부분은 그렇다는 이유로 점수가 꽤나 낮게 출제되는 문제입니다. 만약에 문제가 파일같은 것을 제공한다면, 대부분은 그 파일을 메모장으로 열거나, 헥스값 에디터, 또는 파일의 속성을 열게 된다면 답이 보입니다. 하지만, 만약에 주어지는 문제에 쓰여있는 것이 수학문제라고 친다면, 답은 복잡하게 생각할 필요 없이 그 수학문제의 답일 수도 있어요. 그러므로 모든 가능성을 고려하며 문제를 풉시다. 어쩔 때는 단순히 이상한(?) 확장자의 파일을 열면 되니 확장자를 구글링해서 툴을 받은 후에 열거나 메모장으로 파일 포맷(이나 헤더)을 찾아 구글링해서 맞는 프로그램으로 열면 대부분은 키값이 나오게 됩니다.

MISC(ELLANOUS) 문제

-MISC문제는 TRIVIA보다는 컴퓨터에 대한 지식이 많이 필요하지 않습니다. 대부분은 컴퓨터에 관한 책, 영화등의 내용이 많이 나오는데, 평소에 많이 알고있으면 좋겠지만 안그렇다면 답이 나올만한 예상 책/영화들과 문제에 나오는 단어들은 같이 구글링하면 답이 나올 때도 있습니다. 이 종류는 가끔은 문제 자체에 많은 힌트들이 있기도 하니 문제 자체를 구글링해도 답이 나옵니다.

※주로 쓰이는 미디어

-Hackers 영화

-아니면 이 섹션은 문제수가 적어 분류할 수 없는 문제들이 배치되어 있습니다(자주 Steganography나 Forensic같은 분야들이 여기에 들어갑니다). 이 문서에서는 기술적인 내용같은 깊은 내용은 넘어가지 않을 것이기 때문에 EXAMPLE 섹션에는 이 경우의 예제는 넣을 것이지만 대회마다 MISC의 기준이 꽤나 다른 종류들보다는 다르고 다양한지라 모든 경우에 대한 내용을 쓸 수가 없는점은 양해 부탁드립니다.

TRIVIA 문제

-TRIVIA문제는 컴퓨터에 대한 지식이 조금 더 필요한 문제입니다. 컴퓨터 역사, 바이러스, 운영체계, 기술, 등의 문제가 많이 나오는데 다행이도 오히려 유명한 내용들이라서 그런지 구글링하면 왠만한 문제들은 타 문제들보다는 풀기 쉽습니다. 대부분은 역시 문제에 나오는 힌트로 유추하면 좋고, 문제에 힌트가 별로 안나온다면 문제 자체를 구글링하거나 문제 제목 자체를 구글링하는것도 좋은 방법입니다. 가끔은 답이 구글 검색결과의 첫페이지가 아니라 마지막 검색 결과일 수도 있으니 검색 결과를 모두 훑어보는게 좋은 방법입니다.

※주로 쓰이는 미디어

-세상의 많은 바이러스들(날짜/피해/이름/사용한 툴..등등)
-역사적으로 남는 큰 사건들

RECON(STALKING) 문제

-RECON문제는 요즘 많이 사용되기 시작하는 문제로써, 스토킹이 쉬워지는 요즘 사회를 사용하는 방법을 알려주는 문제입니다. 사회공학 해킹이라고 볼 수도 있겠죠.
대부분은 사용자의 이름이나 정보, 혹은 블로그같은 링크를 주는데요, 거기서 정보를 얻어내야합니다.

많은 방법중 하나는, 홈페이지가 나왔다면 홈페이지를 후이즈를 하거나, 혹은 블로그 프로필을 봅니다. 주어진 정보가 한 사람의 이름이거나 닉네임이라면 그 닉네임을 구글링하거나 닉네임 유무사이트에 가서 그 아이디가 가입되어 있는 사이트들을 찾아 확인해봅니다. 많은 레콘 문제들은 컴퓨터 관련 커뮤니티에 답이 있는 경우가 많으므로 컴퓨터 관련 커뮤니티가 뜬다면 그것은 반드시 체크합니다. 여기서 체크한다는 것은 그저 접속만 해보는것이 아니라 그 페이지에 있는 거의 모든 탭을 다 열어보는 것을 뜻합니다. 가끔은 한 홈페이지의 서브디렉토리를 찾아보는 방법도 좋은 방법입니다.

팁- 가끔은 구글링 하면 해당 대회의 전 회에 나왔던 문제들의 라잇업이 뜨기도 하는데, 이 라잇업들은 오히려 문제 풀때 헷갈리게 하고 자꾸 참고하게 되니 '그냥 이런 유형도 나오는구나' 라고 보시기만 하면 됩니다.

※주로 쓰이는 미디어

-reddit.com
-youtube.com
-whois.com

★EXAMPLES☆

이 부분은 문제들을 각각 유형마다 모아놓은 곳입니다. MISC종류에서 나오는 문제들을 보실 수 있습니다.

BONUS 문제 Example)

문제출처: http://xcz.kr/ [xcz.kr Prob 20- Bonus Problem!]

-문제: [사진]

-열어보면 랜덤한 사진이 한장 있습니다. 하지만 제목에서 보이듯이, 이 문제는 컴퓨터에 대한 깊은 지식이 필요하지 않습니다! 점수에서도 보이고요. 그렇다면 사진을 가지고 놀아봅시다. 메모장으로도 열어보고, 헥스에디터로도 열어보고 그래도 아무것도 안보인다면 속성을 열어봅니다. 속성에 키값이 있습니다.

문제 출처: http://play.newheart.kr/ [NewHeart WhiteHat Prob 05- Bonus100]

-문제: [사진]

-여기서 제공되는 사진은 사칙연산이 마구 쓰여있네요. 메모장으로 열어보고, 속성도 열어보고, 했는데 아무것도 안나옵니다. 그렇다면? 보이는 그대로 숫자들을 연결해 사칙연산을 해줍니다. 그렇게 해서 나오는것이 키값입니다.

MISCELLANOUS 문제 Example)

문제출처: http://forbiddenbits.net [ForbiddenBITS CTF MISC- Unnnnlucky]

참고 라잇업: http://pwnies.dk/post/charsheet-unnnnlucky-plaidctf-2013/

-문제: Where does The Plague hide his money?

-The Plague는 “Hackers” 영화에 나오는 악당입니다. The Plague가 해커스에서 나오는 인물이라는 것을 할게되면, 관련 대본이나 동영상을 찾아봅니다. 라잇업에서 보면, “이것때문에 유투브에서 해커스 영화 조각조각을 찾아 11개는 본것 같다. 답은 03087-08351-27H 라는 계정이었다”, 라고 합니다. 이처럼 MISC문제는 노가다와 집중력이 필요한 문제들입니다.

문제출처: http://yut.codegate.org/ [Codegate 2013 prequals Misc 100]

참고 라잇업: http://goo.gl/Hr5VQV

-문제: ANGELA BENNETT LOGIN UNITED STATES DEPT. OF ENERGY ATOMIC ENERGY COMMISSION. What is login password?

-Angela Bennett이 나온 영화인 “The Net” 에 비밀번호가 나온다고 합니다. 자막을 뒤지면서 ‘비밀번호’라는 단어를 찾아보았더니 한순간에 나왔다고 해요. 영화에 등장했던 비밀번호가 문제의 키값이 된 것이죠.

문제출처: https://ctf.isis.poly.edu/ [CSAW 2013 Misc 200- deadbeef]

참고 라잇업: http://goo.gl/2wF9bY

-문제: [사진](위의 블로그에 있습니다)

-이 문제는 위에 말한 ‘기타’로 분류된 문제입니다. PNG파일이 주어지고, 사이즈를 줄였기 때문에 밑의 글씨가 나오지 않는데 크기 부분을 수정해 화이트보드가 다 나오도록 수정하면 키값이 나온다고 합니다. 고로 스테가노그래피/포렌식 문제라고 할 수 있습니다.

TRIVIA 문제 Example)

문제출처: https://ctf.isis.poly.edu/ [CSAW 2013 Trivia 50]

-문제: Drink all the booze, ____ all the things!

-구글에 Drink all the booze, ____ all the things! 를 치면 자동완성이 완성해 줍니다. Drink all the booze, hack all the things! Hack가 키값입니다.

문제출처: http://ctf.nullcon.net/ [Nullcon HackIM 2013 Trivia 500]

참고 라잇업: http://goo.gl/RBCduS

-문제: What is the first 4 bytes in a neXT fat binary?

-구글에서 neXT fat binary magic를 검색하여 나오던 사이트들을 뒤지던중 http://goo.gl/ODXjJy 이 사이트에서 나오는 정보 중 **“cafe babe # Fat Binary Magic Number #”** 라는 문단에서 정답을 알아낼 수 있었다고 합니다.

RECON(STALKING) 문제 Example)

문제출처: https://ctf.isis.poly.edu/ [CSAW 2013 Recon- historypeats 100]

-문제: https://www.google.com/search?&q=historypeats

-문제가 바로 구글로 유도해줍니다. 바로 위에 깃허브 페이지들이 많이 보이는데요, 그 중 요즘에 활동한 내역에서 댓글을 지운 내역이 보여집니다. 지워진 댓글의 내용을 확인해보니 바로 키값이 나옵니다.

문제출처: http://whitehatcontest.ls-al.org/ [Whitehat Cont. - Stalking 100]
-문제: http://ls-al.org 사이트를 전체적으로 관리하고 있는 숨겨진 진짜 운영자는 누구인가? 정보의 바다, 인터넷을 통한 '합법적' 뒷조사로 운영자의 실제 이름을 알아내시오.
-합법적인 뒷조사를 하라고 합니다. 그렇다면, whois.com으로 가 ls-al.org의 도메인을 소지하고 있는 사람의 정보를 찾아봅니다. 전화번호인 02-5882-1004가 눈에 띄는데요, 이를 구글에 검색하게 되면 한 블로그의 프로필이 보입니다. 그 블로그 주인의 닉네임이 키값입니다.

끝마치며)잡담

처음에는 그냥 재미로 “아, Misc에 대한 문서는 어떨까? 재밌겠다" 라고 시작한걸 정말로 쓰게 될 줄은 몰랐습니다. 그래도 반 재미, 반 정리 차원에서 쓴 글이니 조금 많이 부족하긴 하더라도 재미있게 읽어주셨으면 좋겠습니다. 쓰는건 재미있었어요ㅋㅋ
Misc문제는 모든 사람들의 기준이 달라서 조금 쓰는데 까다롭고 애매했는데, 그래서 중간에 여러번 다 지울까도 많이 고민하게 됐었는데 어느새 그냥 써버리게 됐네요.. 이 문제들은 언제나 오픈마인드를 가지는게 중요한 것 같습니다. 여기 적힌 방법들 말고도 무궁무진한 가능성이 있으니 모든 가능성을 생각해보셔야 해요 :) 문제의 의도도 다양하고 풀이법도 많아 노가다도 들고 어려운 분야이긴 하지만.. 타 분야만큼 기술적이진 않더라도 재미있다고 생각해요.

예제 찾는게 가장 재미있었네요ㅋㅋ 개인적으로 기억에 남는 Misc 문제들이 많았기에 가능했던 것 같습니다. 다시 읽어보니 번역기로 돌린것 같은 딱딱한 문장들이 많이 보이는데 죄송합니다.. 제 한국어 구사 능력의 한계가 보이네요..ㅠㅠ 양해해주세요

그럼 Misc 즐겁게 푸시길 바랍니다~