# 보안용어 정리

정보보호 vs 정보보안

정보보호: 정보의 수집 가공 저장 검색 송신 수신 중에 정보의 훼손 변조 유출 등을 방지하기 위한 관리적/기술적 수단을 강구하는 것

정보화 역기능을 방지하기 위하여 정보 및 정보시스템을 보호하고,정보의 비밀성,무결승,인증,부인봉쇄,가용성을 보장해 줄 수 있도록 관리적,물리적,기술적 수단을 강구하는 것

정보보안

비밀성에 초점을 맞추어 기업의 영업비밀이나 개인의 프라이버시를 보호하기 위해서 주로 사람에 의하여 고의적으로 발생하는 정보의 유출 도청 파괴에 대한 대응을 강조하는 것..

🡪비밀성 유지에 초점을 맞춘 보안의 개념에 상당히 치우쳐 있음

정리

-정보보호; 보호해야 할 가치가 있는 정보를 외부의 위협으로부터 지키는 활동

Ex)개인정보

-정보보안;지정된 일부의 인원만 알고 있어야하는 정보를 위험으로부터 지키는 것

Ex)시스템 보안,db보안,소스코드 보안

COMPUTER FORENSIC VS DIGITAL FORENSICS

Computer forensic

자료의 무결성을 유지하는 방식으로 조사 목적으로 컴퓨터 관련 자료를 수집, 보존, 분석하는 관행.

Digital Forensics

정보의 무결성을 보존하고 데이터에 대한 엄격한 보호 체인을 유지하는 동시에 데이터의 식별, 수집, 검사 및 분석에 과학의 적용.

정보의 공급자가 제공한 정보를 관리하는 경우

-스푸핑

🡪유명 사이트 메일을 도용하여 스팸메일을 보내 수신자로 하여금 해당 메일을 열어보게끔 유도하는 행위

-스니핑(킁킁 냄새를 맡다)=”도청”

=다른 상대방의 패킷을 엿 봄.ID나 패스워드 등 네트워크상에 자신이 아닌 상대방들의 패킷을 훔쳐보는 것

-스누핑(기웃거리다,염탐하다)

스니핑과 같이 도청.

네트워크상에 떠도는 중요 정보를 몰래 획득하는 행위

스미싱

문자 메시지를 보내어 URL링크를 통해 악성코드 설치 후 개인정보 탈취 및 원격 조종

당신이 알아야 할 16지 보안용어

Cloud

요청을 원격으로 처리하는 대용량 저장소 기능을 가진 컴퓨터들의 모음입니다

Vpn

위치를 가리고 트래픽을 암호화하여 인터넷을 사용하면서 익명으로 남길 수 있는 도구.

Exploit

컴퓨터의 취약성을 이용하는 데 사용할 수 있는 악성 애플리케이션 또는 스크립트.

방화벽 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템

멀웨어

(=악성코드)

피싱

전자우편 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장함으로써, [비밀번호](https://ko.wikipedia.org/wiki/%EB%B9%84%EB%B0%80%EB%B2%88%ED%98%B8) 및 [신용카드](https://ko.wikipedia.org/wiki/%EC%8B%A0%EC%9A%A9%EC%B9%B4%EB%93%9C) 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 social engineering의 한 종류

# 악성코드의 종류

# Virus

트로이얀(Trojan)과는 달리 스스로를 복제, 특정한 대상(파일, 부트 섹터 등)을 감염시켜서 해당 대상이 실행되면 동작하는 악성코드

## 트로이 목마(trojan)

[컴퓨터 바이러스](https://namu.wiki/w/%EC%BB%B4%ED%93%A8%ED%84%B0%20%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4)와 다른 점이 있다면, 다행히도 바이러스와 달리 살아있는거 마냥 다른기기를 전부 전염시키고, 자가복제를 하거나 다른 정상적인 파일에 자기 자신을 덮어 씌우거나 하지 않고, 해당하는 트로이 목마 프로그램 하나만 삭제하면 더 이상의 피해는 없다.

### 스파이웨어

중요한 [개인정보](https://namu.wiki/w/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4) 등을 수집하고 공격자의 서버로 전송

### 백도어

백도어는 말 그대로 뒷문이라는 뜻으로, 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용 프로그램 또는 시스템에 접근하여 컴퓨터 속의 정보를 빼내가거나 특정 작업을 하도록 제작된 프로그램

### 랜섬웨어

컴퓨터의 데이터에 암호를 걸고, 데이터를 인질로 삼아 잠금을 해제하는 키를 대가로 금품을 요구하는 악성코드

리버싱 -> 바이너리(Binary)

어느 특정 물건, 장치 등이 있으면 그것에 대한 구조, 기능, 동작 등을 역으로 따라가며 분석하고 그 원리를 이해하며 부족한 부분을 보완하며 새로운 기능 등을 추가하는 작업

제로데이 헌팅:  [컴퓨터](https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0) [소프트웨어](https://ko.wikipedia.org/wiki/%EC%86%8C%ED%94%84%ED%8A%B8%EC%9B%A8%EC%96%B4)의 [취약점](https://ko.wikipedia.org/wiki/%EC%B7%A8%EC%95%BD%EC%A0%90)을 공격하는 기술적 위협

* 악성코드: **악성코드**([Malware](https://namu.wiki/w/%EB%A9%80%EC%9B%A8%EC%96%B4), 악성 소프트웨어)는 컴퓨터 바이러스, 웜, 스파이웨어, 트로이 목마 등 컴퓨터 사용자에게 해를 끼치는 모든 코드(Code)의 총칭을 말한다.

[기계어](https://ko.wikipedia.org/wiki/%EA%B8%B0%EA%B3%84%EC%96%B4)와 일대일 대응이 되는 [컴퓨터](https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0) [프로그래밍](https://ko.wikipedia.org/wiki/%ED%94%84%EB%A1%9C%EA%B7%B8%EB%9E%98%EB%B0%8D)의 [저급 언어](https://ko.wikipedia.org/wiki/%EC%A0%80%EA%B8%89_%EC%96%B8%EC%96%B4)이다.

|  |
| --- |
| ----------------------------------------------------------------------------------------  **< 리버싱 >**  1. 리버싱 핵심원리    처음부터 끝까지 공부하면 지루하고 이해도 안되기때문에  DLL인젝션 전까지만 확실하게 하시고 그 뒤 부터는 나중에 보셔도됩니다.  .  2. simples.kr  여기가면 시즌1 문제랑 시즌2 문제 있습니다  기초 다지는데 좋습니다  write up도 있구요  3. <http://codeengn.com/>  한국 리버싱 사이트중 하나입니다.  Basic RCE 20개 부터 차근차근 풀어봅니다  그 뒤에 Advanced를 풀든 뭘 풀든 아무거나 풉니다.  추가> [https://tuts4you.com/download.php?list.17](http://tuts4you.com/download.php?view.2876)  tuts 4 you 사이트입니다.  여기에 레나님의 초보자를 위한 리버싱 40개 있는데  동영상 강의도 있고 굉장히 좋습니다.  동영상 강의보면서 40개 풀면 초보자는 탈출할 수 있을겁니다  4. <https://tuts4you.com/download.php?list.49>  tuts 4 you 챌린지입니다.  각 종 문제들 풀면서 실력을 늘립니다.  추가> <http://crackmes.de/>  거의 모든 리버싱 문제가 모여있습니다...  2000개 넘게 있으니 앞에있는 문제 다풀고 풀거 없을 때 풀어보면 좋습니다.  추가 > <http://reversing.kr/>  리버싱 문제 난이도가 높다고 합니다.  아직 안풀어봐서 모르겠습니다ㅠㅠ  여기 까지 하셨으면 악성코드 분석하시면 됩니다  자기 혼자 샘플 수집하고  분석하고...하면 하시면됩니다  악성코드 분석 자료 링크  - <http://sinun.tistory.com/95>  - <http://fumalwareanalysis.blogspot.kr/p/malware-analysis-tutorials-reverse.html?m=1>  - <http://carpedm20.blogspot.kr/2012/08/bundestrojaner.html>  - <http://espionageware.blogspot.kr/>  스타크래프트 시디키 알고리즘 분석 자료 링크 - <http://carpedm20.blogspot.kr/2012/08/blog-post_7630.html>  리버싱 관련 모든 서적들 입니다.  **쉬어가기**  **악성코드, 그리고 분석가들**  <http://book.naver.com/bookdb/book_detail.nhn?bid=6589104>    **초급**  **리버스엔지니어링 - 역분석구조와원리**  <http://book.naver.com/bookdb/book_detail.nhn?bid=4751209>    **중급**  **리버싱 핵심원리**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7009755>    **리버스엔지니어링 바이블**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7001854>    **악성코드와 멀웨어 포렌식**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7016720>    **Application Hacking 애플리케이션 해킹**  <http://book.naver.com/bookdb/book_detail.nhn?bid=6030865>    **해킹의 꽃 디스어셈블링**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7387113>    **고급**  **리버싱 - 리버스엔지니어링 비밀을 파헤치다**  <http://book.naver.com/bookdb/book_detail.nhn?bid=6015339>    **리버싱윈도우**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7285611>    **루트킷 - 윈도우 커널 조작의 미학**  <http://book.naver.com/bookdb/book_detail.nhn?bid=4298506>    **실전 악성코드와 멀웨어 분석**  <http://book.naver.com/bookdb/book_detail.nhn?bid=7327943>    **악성코드 분석가의 비법서**  <http://book.naver.com/bookdb/book_detail.nhn?bid=6892174>    **THE IDA PRO BOOK**  <http://book.naver.com/bookdb/book_detail.nhn?bid=6977530> |

시스템 -> 포너블(Pwnable)

🡪일반 유저의 자격으로 여러가지 공격 기법을 활용해 관리자 자격을 뺏는 것

ASLR은 Address Space Layout Randomization의 약자로, 그 이름에서 알 수 있듯이 자세히 말하면 '실행 및 호출 할 때 마다 주소 배치를 무작위로 배정하는 기법

* DEP와 NX는 둘 다 같은 개념의 보호기법으로 각각 Data Execution Protection과 Non executable의 약자입니다 한 ‘heap과 stack과 같이 buffer overflow 공격에 이용되는 메모리 공간에 있는 코드를 실행시키지 않는 기법
* 버퍼 오버플로우:  [프로세스](https://ko.wikipedia.org/wiki/%ED%94%84%EB%A1%9C%EC%84%B8%EC%8A%A4)가 [데이터](https://ko.wikipedia.org/wiki/%EB%8D%B0%EC%9D%B4%ED%84%B0)를 [버퍼](https://ko.wikipedia.org/wiki/%EB%B2%84%ED%8D%BC)에 저장할 때 프로그래머가 지정한 곳 바깥에 저장하는 것
* 리눅스 환경에서 많이 진행됨
* 1.    C 언어 해석능력
* 2.    프로그램 메모리 구조
* 3.    약간의 리눅스 지식
* 4.    약간의 리버싱 지식

5.    쉘 코드(Shell Code)        -> 이건 굳이 제작법까지 알 필요는 없다고 생각한다. 잘하시는 분들이 다 인터넷에 올려놓으셨다 1. <http://carpedm20.blogspot.kr/2013/07/blog-post_28.html>  
  
백트랙의 기본적인 활용법과 metasploit 명령어 정보를 정리한 ppt 자료  
  
2. <http://www.hackerschool.org/Sub_Html/HS_University/BOF/essential/00.html>  
  
상당히 어려운 BOF 기법을 기초부터 시작해서  
차근차근 알려주는 강좌입니다.  
BOF에 관심이 없으시더라도 꼭 한번 읽어보시기 바랍니다.  
  
3. <http://www.securitytube.net/video/1175>  
  
시스템 해킹을 실습해 볼 수 있게 해주는 Metasploit 강좌입니다.  
참고로 Backtrack이랑 Metasploit은 동영상 강좌로  
배우시는게 제일 빠릅니다.  
유투브에 검색하시면 정말 많은 강좌들이 있으니 참고하시기 바랍니다.  
  
4. <http://www.offensive-security.com/metasploit-unleashed/Main_Page>  
  
Metasploit을 만든 회사에서 지원하는 튜토리얼입니다.  
  
튜토리얼 중 msfconsole 부분 번역 :  
<http://carpedm20.blogspot.kr/2012/08/metasploit-unleashed-msfconsole.html>  
<http://carpedm20.blogspot.kr/2012/08/metasploit-unleashed-msfconsole-2.html>  
<http://carpedm20.blogspot.kr/2012/08/metasploit-unleashed-msfconsole-3.html>  
  
5. <http://www.hackingdna.com/>  
  
Backtrack 에서 사용할 수 있는 툴들의 사용법이 상당히 많은 블로그 입니다.  
스캔, 스니핑, 크랙, 파일 받기, 보내기, 스샷 찍기, 웹캠 실행 등..  
여러분들의 환상은 Backtrack을 통해 충분히 채우실 수 있을겁니다.  
Backtrack을 vmware에 설치하셔서 가상 환경에서만  
실습하시기 바랍니다. (해킹은 불법입니다.)

6. <http://www.hackingarticles.in/best-of-metasploit-meterpreter-script-meterpreter-cheat-sheet/>  
  
meterpreter 에서 자주 사용하는 명령어 입니다.  
meterpreter 는 메타스플로잇에서 제공하는 공격 쉘로,  
exploit이 성공한 후 타겟과 통신할 때 사용하됩니다.  
  
7. <http://youtu.be/YFoWDETyrYg>, <http://youtu.be/ljnzQoE0KFc>  
  
메타스플로잇을 이용해서 윈도우7 해킹 시연 영상입니다.  
자세한 명령어의 사용은 나와 있지 않지만, 백트랙과 메타스플로잇으로  
해킹을 한 후 어떤 것들을 할 수 있는지 대략적으로 감을 잡으실 수 있습니다.  
다시 한번 강조하지만, 해킹은 불법이며,  
모의 해킹을 위해서만 해킹을 시연하시기 바랍니다.  
  
8. <http://blog.naver.com/PostView.nhn?blogId=ka0r1&logNo=90165963416&redirect=Dlog&widgetTypeCall=true>  
  
쉘 코드 작성 강좌입니다.  
상당히 긴 글이지만, 그만큼 자세하게 쉘 코드를 작성하는 방법을 설명한 글입니다.  
  
9. <http://www.hackerschool.org/HS_Boards/view.php?id=Lib_system&page=1&sn1=&divpage=1&sn=off&ss=on&sc=on&select_arrange=hit&desc=desc&no=100>  
  
BOF의 기초를 알려주는 강좌입니다.  
hackerschool BOF 강좌 보시고나서 보시면 이해도 잘되고  
BOF에 대해 정말 많은걸 얻으실 수 있을겁니다.  
  
10.[http://devanix.tistory.com/129](http://devanix.tistory.com/entry/BOF-%EC%9B%90%EC%A0%95%EB%8C%80-%EC%B6%9C%ED%95%AD-%EC%A4%80%EB%B9%84-%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC-%EC%84%A4%EC%A0%95)  
  
BOF 원정대라고, BOF를 실습해 볼 수 있는 워게임이 있는데  
그 워게임에 대한 강좌입니다.  
BOF 이론 공부부 하시고나서 꼭 한번 실습해 보시기 바랍니다.

11. <http://s3ize.blogspot.kr/2012/08/load-of-bof-level1.html>  
  
또 다른 BOF 원정대 풀이가 있는 블로그 입니다.  
버퍼 오버플로우는 한두번 봐서는 이해가 잘 안되기 때문에  
여러군데의 풀이를 보시면서 이해를 하시기 바랍니다.  
  
12. <http://5a5in.com/wordpress/?p=1107>  
  
BOF 원정대 풀이가 있는 다른 블로그 입니다.  
  
13. <http://geundi.tistory.com/118>  
  
버퍼 오버플로우에 대한 개념을 이해하기 쉽게 설명해 놓은 글 입니다.  
스택에 대해 아주 자세히 설명이 되어 있고, 그림도 많기 때문에  
이해하기 쉬울거라 생각됩니다.  
  
14. <http://www.hackerschool.org/HS_Boards/data/Lib_system/omega1.txt>  
<http://www.hackerschool.org/HS_Boards/data/Lib_system/omega2.txt>  
  
스택 오버플로우 할 때 마다 복잡한 계산을 덜 수 있는  
'오메가 프로젝트' 번역 문서입니다.

15. <http://sinun.tistory.com/156>

흔하지 않은 윈도우 공격 코드 작성 튜토리얼 번역글 입니다.

원본 글은 <https://www.corelan.be/> 이 곳에서 작성되었고,

[exploit-writing-tutorial-part-1-stack-based-overflows](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/) 가 원본 글 입니다.  
  
윈도우에서 공격이 왜 가능하고, 어디에서 공격을 시도해야 하며  
어떻게 공격 코드를 짜는지 까지 설명해 놓은 문서입니다.  
메타스플로잇에서 사용되는 exploit 들이 어떻게 만들어 지는지  
대략적으로 감을 잡으실 수 있을거라 생각됩니다.  
exploit에 관심이 있으신 분은 꼭 한번 읽어보시기 바랍니다.

16. <http://cdpython.tistory.com/28>  
  
위에 소개한 exploit-writing-tutorial-part-1-stack-based-overflows 의 다른 번역글입니다.  
  
17. <http://www.punter-infosec.com/exploit-writing-tutorials-for-pentesters/>  
  
exploit-writing-tutorial-part-1-stack-based-overflows 뿐만 아니라  
공격 코드를 작성하는 방법을 설명한 튜토리얼을 모아둔 글 입니다.  
  
18. <http://hyunmini.tistory.com/13>  
  
작성된 공격 코드를 어떻게 메타스플로잇에서 사용할 수 있는지를  
설명한 글 입니다. 위의 튜토리얼에서 작성하신 코드들을  
메타스플로잇을 통해 쉘을 얻을 수 있는 코드로 바꿀 수 있을 것 같습니다.  
  
19. [Win32 Attack Local Shellcode 작성방법 [달고나]](http://www.google.com/url?sa=t&rct=j&q=Win32+Attack+1.+local+shellcode&source=web&cd=1&ved=0CDMQFjAA&url=http%3A%2F%2Fwowhacker.com%2Fboard.php%3Fbid%3D174%26bs_type%3D%26bs_str%3D%26cate%3D0%26pg%3D0%26mode%3Dfiledown%26puid%3D163512%26uid%3D19&ei=AKhnUbveJIm6lAXWvoGQBA&usg=AFQjCNGXwXm1LcjapVkuv_UJfYzmvq-80Q&sig2=YnY1tt52OVtelipox0JJQQ&bvm=bv.45175338,d.dGI&cad=rja)  [Win32 Attack 2. Local Buffer Overflow](http://www.google.com/url?sa=t&rct=j&q=Win32+Attack+1.+local+shellcode&source=web&cd=2&cad=rja&ved=0CDoQFjAB&url=http%3A%2F%2Fwowhacker.com%2Fboard.php%3Fbid%3D174%26bs_type%3D%26bs_str%3D%26cate%3D0%26pg%3D0%26mode%3Dfiledown%26puid%3D163519%26uid%3D20&ei=AKhnUbveJIm6lAXWvoGQBA&usg=AFQjCNF5sDz-CZaaHpDeRvWomy-6FM2R4Q&sig2=ZMzSwbEb1sBfRicOx7x-uQ&bvm=bv.45175338,d.dGI)  
  
윈도우 기반 쉘코드 작성 튜토리얼 문서입니다.  
  
20. <http://exploit-exercises.com/>  
  
BOF 원정대와는 다른 시스템 해킹 워게임 사이트 입니다.  
해외 사이트이며, 난이도 별로 vmware 이미지를 제공합니다

웹해킹 -> 웹해킹(WebHacking)

* 비교적 진입장벽이 낮은 편
* [file:///D:/%EB%8B%A4%EC%9A%B4%EB%A1%9C%EB%93%9C/Webhacking.kr%EC%9D%84%20%ED%86%B5%ED%95%B4%20%EB%B0%B0%EC%9A%B0%EB%8A%94%20%EC%9B%B9%20%ED%95%B4%ED%82%B9.pdf](file:///D:\%EB%8B%A4%EC%9A%B4%EB%A1%9C%EB%93%9C\Webhacking.kr%EC%9D%84%20%ED%86%B5%ED%95%B4%20%EB%B0%B0%EC%9A%B0%EB%8A%94%20%EC%9B%B9%20%ED%95%B4%ED%82%B9.pdf)
* XSS

[웹 애플리케이션](https://ko.wikipedia.org/wiki/%EC%9B%B9_%EC%95%A0%ED%94%8C%EB%A6%AC%EC%BC%80%EC%9D%B4%EC%85%98)에서 많이 나타나는 취약점의 하나로 [웹사이트](https://ko.wikipedia.org/wiki/%EC%9B%B9%EC%82%AC%EC%9D%B4%ED%8A%B8) 관리자가 아닌 이가 [웹 페이지](https://ko.wikipedia.org/wiki/%EC%9B%B9_%ED%8E%98%EC%9D%B4%EC%A7%80)에 악성 [스크립트](https://ko.wikipedia.org/wiki/%ED%81%B4%EB%9D%BC%EC%9D%B4%EC%96%B8%ED%8A%B8_%EC%82%AC%EC%9D%B4%EB%93%9C_%EC%8A%A4%ED%81%AC%EB%A6%BD%ED%8A%B8)를 삽입할 수 있는 취약점

* PHP,CGI 기반 게시판 같은 것들을 많이 만들어보면 도움이 됨
* [기술 종류](http://hackwiki.maru.net/doku.php?id=webhack:%EA%B8%B0%EC%88%A0_%EC%A2%85%EB%A5%98)
* SQL INJECTION: 클라이언트의 입력값을 조작하여 서버의 [데이터베이스](https://namu.wiki/w/%EB%8D%B0%EC%9D%B4%ED%84%B0%EB%B2%A0%EC%9D%B4%EC%8A%A4)를 공격할 수 있는 공격방식
* 1. <http://webhacking.kr/>
* 가장 유명한 워게임. 난이도가 고루 분포되어 있습니다.
* 여기 문제의 대부분을 푸셨다면, 더 이상 이런 글들을 보지 않으셔도 될겁니다.  
    
  2. <http://suninatas.com/>  
    
  webhacking.kr 보다는 쉽다고 평가되는 워게임 사이트 입니다.  
    
  3. <http://www.hackthissite.org/>  
    
  해외에서 유명한 워게임  
  난이도가 쉬운편이며, 해외에서 많이 유명하기 때문에 그만큼 풀이도 많이 있습니다.  
    
  4. <http://www.hacker.org/>  
    
  독특한 워게임. 위의 워게임들과는 스타일이 조금 다릅니다.  
    
  5. <http://tools.web-max.ca/encode_decode.php>  
    
  워게임 푸실때 자주 이용되는 사이트.  
  url, base64, base85 등 인코딩, 디코딩 사이트입니다.  
    
  6. <http://tools.web-max.ca/encode_decode.php>  
    
  웹 문제 풀 때 이외에도 crypto 문제가 나올때 자주 이용하는 사이트.  
    
  7. <http://totoriver.egloos.com/3403564>  
    
  웹 해킹 관련 글 많은 블로그입니다.  
  상당히 좋은 정보들을 많이 공유하시고, webhacking.kr 도메인 소유자인듯 보입니다.  
    
  8. <https://lael.be/84>  
    
  웹 해킹에서 가장 많이 사용되는 sql 인젝션을 설명한 글 입니다.  
  공격 쿼리가 어떻게, 왜 작성되는지에 대한 정보를 얻으실 수 있을겁니다.  
    
  9. [lael.be/attachment/1109936462.pdf](http://lael.be/attachment/1109936462.pdf)  
    
  기초적인 db의 구조에 대한 설명을 시작으로  
  인젝션 쿼리를 어떻게 만들 수 있는지에 대한 문서입니다.  
  sql 인젝션에 대해 잘 모르시는 분들은 이 문서를 읽는 것부터 시작하면 좋을 것 같습니다.  
    
  10. [Blind Sql Injection – MySQL 5.0](http://www.google.com/url?sa=t&rct=j&q=%EB%B8%94%EB%9D%BC%EC%9D%B8%EB%93%9C+%EC%9D%B8%EC%A0%9D%EC%85%98&source=web&cd=1&ved=0CDEQFjAA&url=http%3A%2F%2Fnoon.tistory.com%2Fattachment%2Fcfile23.uf%401841553F4EA56C7C3BA81B.pdf&ei=J6VnUeSUD4SXkQW5jIDwAg&usg=AFQjCNHfM_KeTGe70ttdVb5Uk07NC8NEOQ&sig2=VtkT-XwpYBb-gEItOjAh9w&bvm=bv.45175338,d.dGI&cad=rja)  
    
  sql 인젝션 중 하나인 블라인드 인젝션을 설명한 문서입니다.  
    
  11. [http://k1rha.tistory.com/entry/Sleep-으로-블라인드-인젝션-걸기-Sleep-for-Blind-Injection](http://k1rha.tistory.com/entry/Sleep-%EC%9C%BC%EB%A1%9C-%EB%B8%94%EB%9D%BC%EC%9D%B8%EB%93%9C-%EC%9D%B8%EC%A0%9D%EC%85%98-%EA%B1%B8%EA%B8%B0-Sleep-for-Blind-Injection)  
    
  블라인드 인젝션시 주로 활용되는 sleep 함수의 사용법을 설명한 글 입니다.  
  sleep 외에도 공격 쿼리가 제대로 작동하는지 확인하는 방법은 다양하므로  
  검색을 통해 찾으실 수 있을겁니다.  
    
  12. <http://coffeenix.net/data_repository/pdf/googledork.pdf>  
    
  구글 해킹에 대해 설명한 문서입니다.  
  검색 엔진인 구글을 통해 어떻게 해킹을 할 수 있는지 설명한 문서입니다.  
  주로 웹해킹의 타겟을 찾을 때 사용될 수 있으며, 구글 검색 실력도 향상될 수 있음
* .

크립토(Crypto)🡪수사쪽 개념

포렌식(forensic)🡪 수사쪽 개념

네트워크(Network)🡪보안분야

가장 단순한 네트워크 해킹 기법으로는 DDoS 공격과 백도어 설치가 있다. 실력 있는 해커는 드물기 때문에 일반인이 접할 수 있는 대부분의 네트워크 해킹 기법은 DDoS, 백도어, 피싱, 사회공학 정도다.

DDos)🡪네트워크 해킹 분야로

대량의 패킷 또는 요청을 생성하여 궁극적으로 목표 시스템을 마비하는 기법

## 디지털 포렌식 종류

시스템 포렌식

네트워크 포렌식

모바일 포렌식

디스크 포렌식

Misc