Hacking & Malware

담당교수 : 신원

대상 : 정보보호학과 3/4학년

과목 : 해킹 및 악성코드 대응

학기 : 2020년 1학기

차례

- **해킹 기술 개요**
  - 해킹의 개념과 동향을 살펴봅시다!
- **악성코드 개요**
  - 악성코드의 정의, 기술 발전에 따른 동향과 전망을 살펴봅시다!
- **해커 수준 및 해킹 기법 분류**
  - 해커 수준을 분류해 봅시다!
  - 주로 사용하고 있는 해킹 기법을 분류해 봅시다!

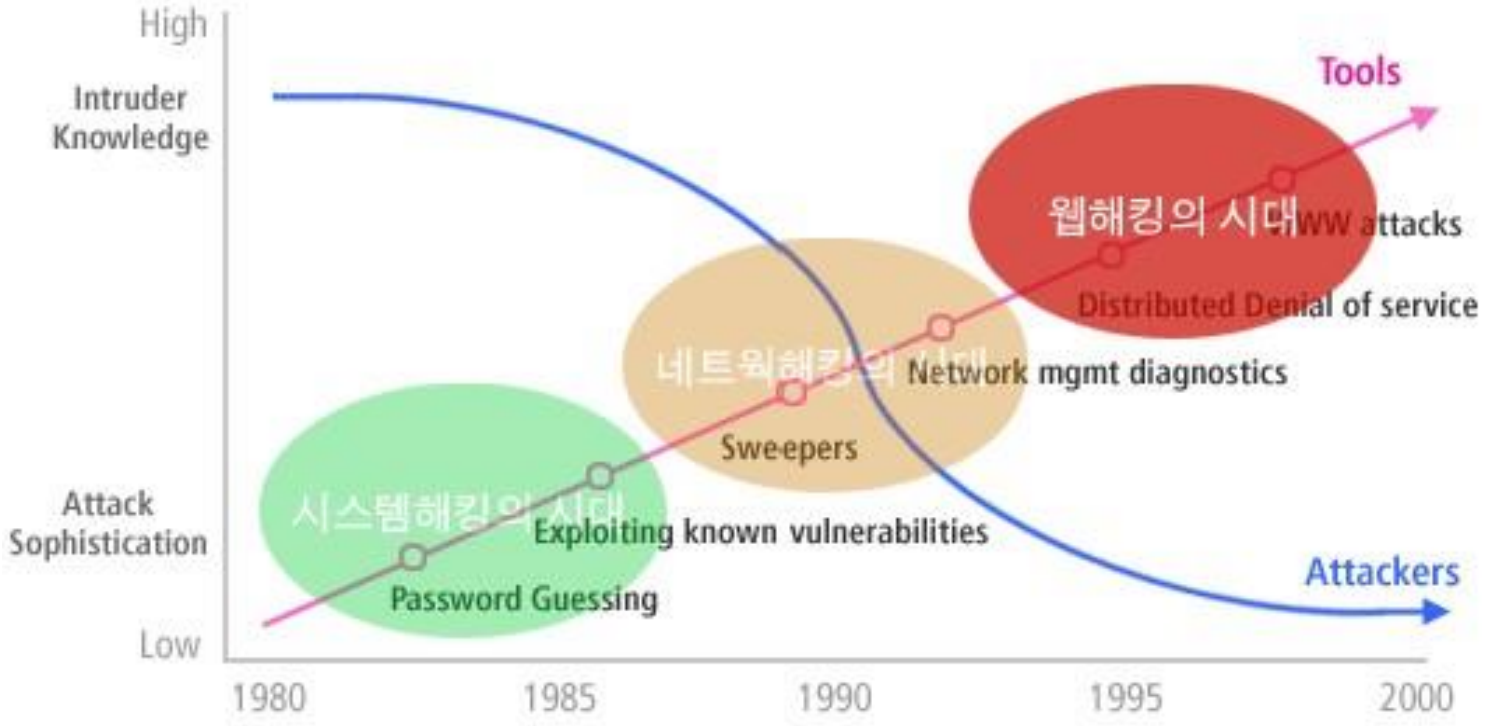
해킹 기술 개요

- **해킹의 일반적 정의**
  - 권한을 부여받지 않은 상태에서 임의의 컴퓨터 시스템에 불법적으로 접근하여 데이터를 빼내거나 파괴하는 행위
  - 단순하게는 컴퓨터 시스템을 대상으로 해커가 하는 모든 행위
- **해커의 정의**
  : Guy L.Steele. et al., The Hacker's Dictionary
  - A person who enjoys learning the details of computer systems and how to stretch their capabilities – as opposed to most users of computers, who prefer to learn only the minimum amount necessary
  - One who programs enthusiastically or who enjoys programming rather than just theorizing about programming

해킹 기술의 발전

"공격도구의 다양화로 해킹 난이도 하락"

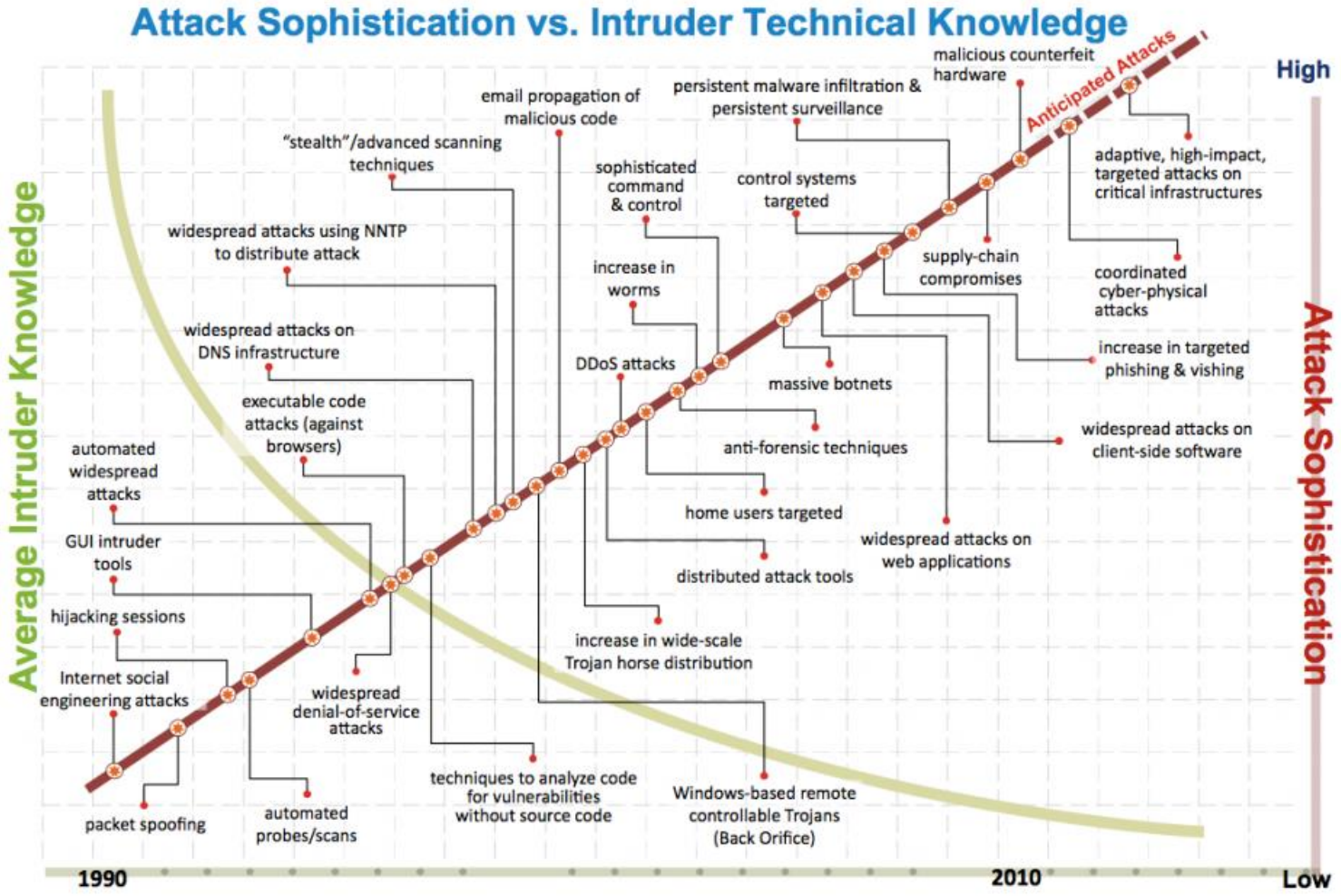
John Pescatore, Security Analyst, Gartner Group



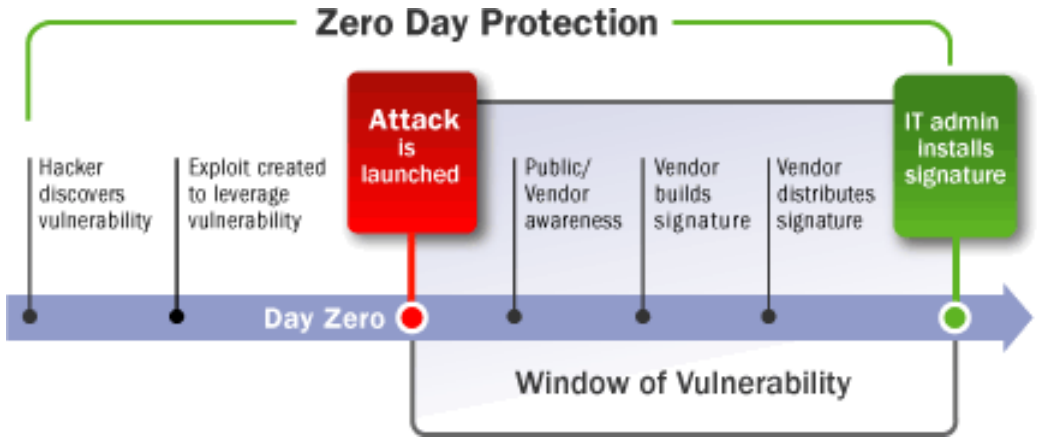
일반적인 해킹 절차

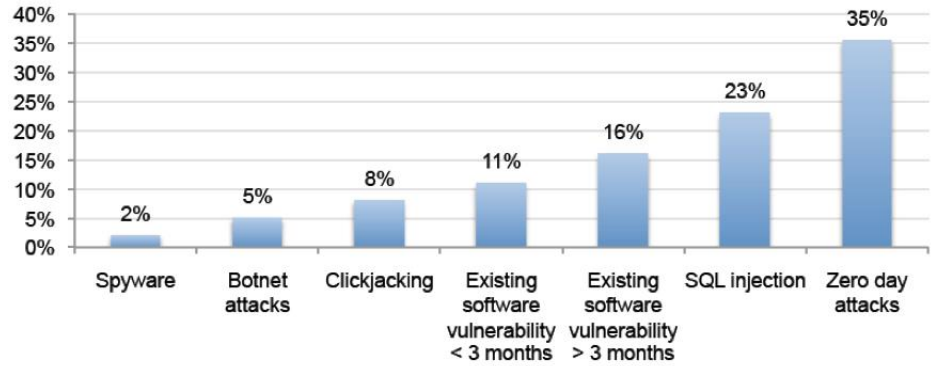
- **네트워크 및 시스템 정보 수집**
  - 네트워크와 시스템을 파악하기 위한 정보 수집 단계
  - 네트워크 구성, 운영체제, 사용 포트 정보, 관리자 및 사용자 정보, 공유자원 정보 등을 수집하고 취약점을 분석
- **시스템 공격 및 침입**
  - 시스템의 가장 취약한 단계를 중심으로 수행되며 다양한 방법들이 동원
  - 시스템 및 네트워크 서비스 상의 버그, 네트워크 도청, 시스템 환경 구성상의 오류 등을 이용하여 침입
- **공격의 확장**
  - 침입의 흔적을 지우거나 백도어를 숨겨두어 다음의 침입을 용이하게 하고, 다른 시스템을 공격하기 위해 준비하는 단계

해킹 기술과 도구의 발전


Attack Sophistication vs. Intruder Technical Knowledge
Average Intruder Knowledge
Attack Sophistication
High
Low
1990
2010
Anticipated Attacks
malicious counterfeit hardware
persistent malware infiltration & persistent surveillance
email propagation of malicious code
"stealth"/advanced scanning techniques
sophisticated command & control
control systems targeted
adaptive, high-impact, targeted attacks on critical infrastructures
widespread attacks using NNTP to distribute attack
increase in worms
supply-chain compromises
coordinated cyber-physical attacks
widespread attacks on DNS infrastructure
DDoS attacks
massive botnets
increase in targeted phishing & vishing
executable code attacks (against browsers)
anti-forensic techniques
widespread attacks on client-side software
automated widespread attacks
home users targeted
GUI intruder tools
widespread attacks on web applications
distributed attack tools
hijacking sessions
increase in wide-scale Trojan horse distribution
Internet social engineering attacks
widespread denial-of-service attacks
techniques to analyze code for vulnerabilities without source code
Windows-based remote controllable Trojans (Back Orifice)
packet spoofing
automated probes/scans

Zero-Day 공격 패턴





eSecurity Planet, 2010

악성코드 개요

- **Lawrence E. Bassham & W. Timothy Polk, “Treat Assessment of Malicious Code and Human Threats”, 1992.**
  - Trojan Horse - a program which performs a useful function, but also performs an unexpected action as well.
  - Virus - a code segment which replicates by attaching copies to existing executables.
  - Worm - a program which replicates itself and causes execution of the new copy.
  - Network Worm - a worm which copies itself to another system by using common network facilities, and causes execution of the copy on that system.

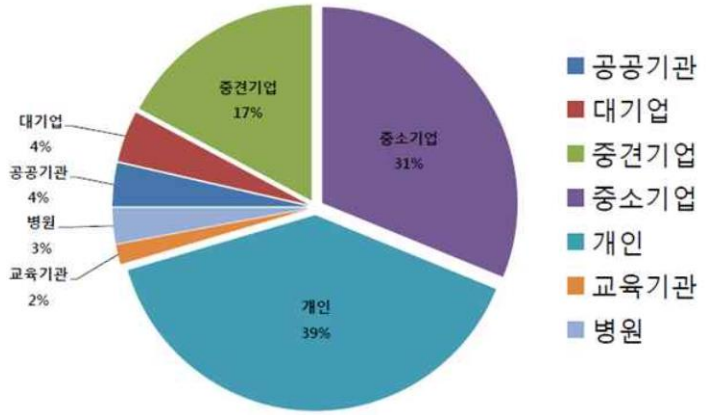
- **악성코드(Malware)의 정의 : 신원**
  - 일반적으로 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의의 목적을 가진 프로그램 및 수행 가능한 매크로, 스크립트 등 실행 가능한 형태의 모든 유형을 포함, 보통 Malicious Code라고도 함
- **Malware의 분류**
  - 복제와 감염을 특징으로 하는 Computer Virus
  - 메모리, 네트워크를 통해 자신을 복제, 배포하는 Worm
  - 자기 복제 능력이 없는 악의의 목적을 지닌 Trojan Horse
  - 브라우저의 설정을 변경하거나 개인 정보를 수집, 전송하는 Spyware
  - 해킹명령 전달 사이트와의 연결로 스팸메일 전송이나 DDoS 공격에 악용이 가능한 Bot
  - 관리자 권한을 획득한 후 커널을 속여서 수행되는 Rootkit
  - 불법으로 설치된 후 사용자 문서 등을 암호화하여 돈을 요구하는 Ransomware
  - 사용자 몰래 악성 코드를 설치하는 Dropper

Virus / Trojan Horse / Worm 비교

- Trojan Horse는 자기 복제가 불가능
- Virus와 Worm은 기생하느냐, 시스템 내에 독립적으로 존재하느냐의 차이

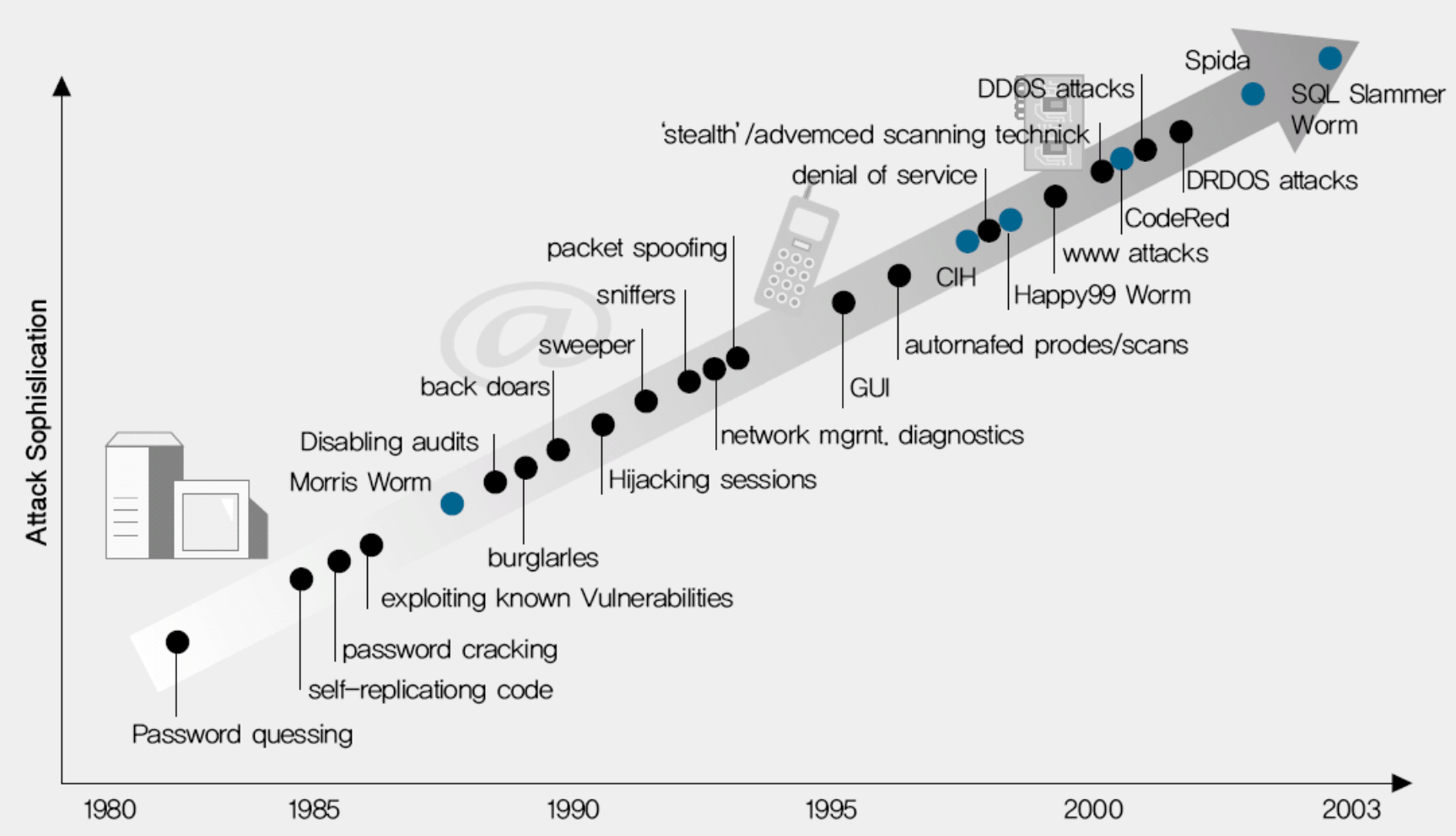
특성 / 종류	자기 복제	감염 대상	형태	복구방법
Virus	O	O	기생/겹침	치료
Trojan Horse	X	X	독립	삭제
Worm	O	X	독립	삭제

Ransomware 감염 업종별 통계 (2016)



이상적인 Ransomware 대응

공격 기술의 발전


Attack Sophislication
1980
1985
1990
1995
2000
2003
Password quessing
self-replicationg code
password cracking
exploiting known Vulnerabilities
burglarles
Morris Worm
Disabling audits
back doars
sweeper
sniffers
packet spoofing
Hijacking sessions
network mgrnt. diagnostics
GUI
autornafed prodes/scans
CIH
denial of service
'stealth'/advemced scanning technick
DDOS attacks
Happy99 Worm
www attacks
CodeRed
DRDOS attacks
Spida
SQL Slammer Worm

백신과 악성 코드에 대한 오해

- 백신을 설치만 해선 악성코드로부터 해방되지 않는다
- 백신의 시스템 감시(실시간 감시)는 악성코드 접근을 차단하지 네트워크를 통한 악성코드의 공격을 예방하지 못한다
- 악성코드가 계속 재발이 꼭 백신의 문제는 아니다 - 공유폴더, 보안 패치 미적용
- 정상적인 파일을 오진할 수 있다
- 제품마다 악성코드 분류가 달라 진단하지 않는 샘플이 존재할 수 있다.
- 백신 하나로 현존하는 모든 악성코드를 진단, 치료할 수 없다
- 시스템의 이상 증세는 모두 바이러스나 웜 때문이 아니다
- 백신도 바이러스에 감염된다

해커 수준 및 해킹 기법 분류

윤리적 측면에서 해커를 분류

분류	내용
Hacker	• Refers to a person who enjoys learning the details of computer systems and to stretch his/her capabilities
Cracker	• Refers to a person who uses his hacking skills for offensive purposes
Hacking	• Describes the rapid development of new programs or the reverse engineering of the already existing software to make the code better and more efficient
Ethical hacker	• Refers to security professionals who apply their hacking skills for defensive purposes

행동양식에 중점을 두어 해커를 분류

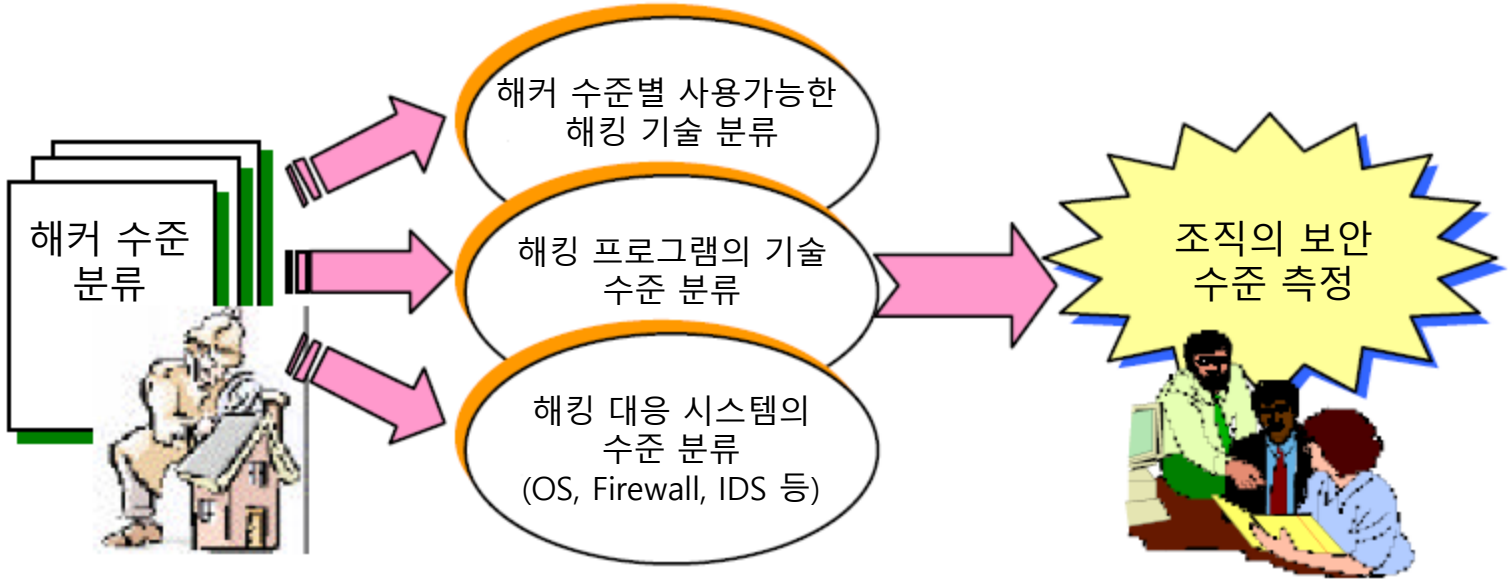
분류	내용
Black Hats	• Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as crackers
White Hats	• Individuals professing hacker skills and using them for defensive purposes. Also known as security analysts
Gray Hats	• Individuals who work both offensively and defensively at various times
Suicide Hackers	• Individuals who aim to bring down critical infrastructure for a "cause" and do not worry about facing 30 years in jail for their actions

구사하는 기술에 중점을 두어 해커를 분류

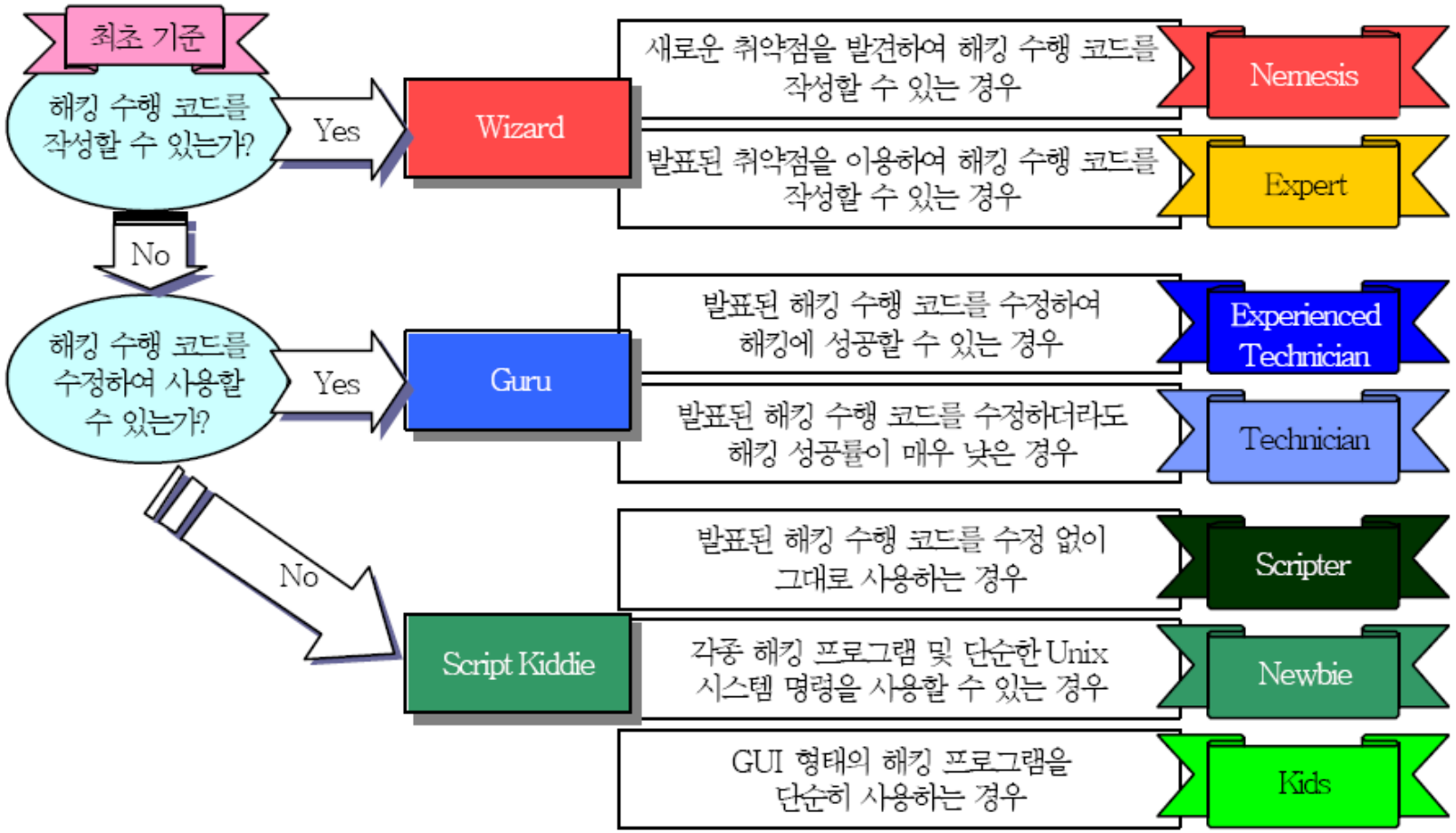
분류	내용
Elite	• 해킹하고자 하는 시스템에 존재하는 취약점을 찾아내고 그것을 이용해 해킹에 성공하는 최고 수준의 해커 • 해킹 시도 목적은 자신이 해당 시스템을 아무런 흔적 없이 해킹할 수 있다는 것을 확인하기 위함
Semi Elite	• 컴퓨터에 대한 포괄적인 지식이 있고 운영체제 시스템을 이해 • 운영체제의 특정한 취약점을 알고 그 취약점을 공격하는 코드를 만들 수 있을 정도의 지식으로 무장
Developed Kiddie	• 보통 십대 후반의 학생들로 대부분의 해킹 기법들에 대해 이해 • 해킹 수행 코드가 적용될 수 있을 만한 취약점을 발견할 때까지 여러 번 시도하여 시스템 침투에 성공하기도 함
Script Kiddie	• 네트워크나 운영체제에 관한 기술과 지식이 부족 • 널리 알려진 트로이 목마를 사용하여 일반 인터넷 사용자를 공격하는 것이 목표
Lamer	• 해커는 되고 싶지만 경험도 기술도 없는 이들 • 네트워크와 운영체제에 관련해 기술적인 지식이 전혀 없는 상태에서 게임과 IRC 채팅, Warez 사이트를 찾거나 크레디트카드 사기 등에 관심이 많음

해커 수준 분류의 목적

- 해커의 수준을 분류함으로써 각 수준의 해커가 사용하는 해킹 기술과 해킹 프로그램(도구)의 기술 수준을 분류하고, 해킹에 대응하기 위한 보안 시스템의 수준을 분류한 후, 모든 것들을 종합하여 해당 조직의 보안 수준을 측정하기 위한 기반 마련 가능



해커 수준 분류와 기준


최초 기준
해킹 수행 코드를 작성할 수 있는가?
Yes
Wizard
새로운 취약점을 발견하여 해킹 수행 코드를 작성할 수 있는 경우
Nemesis
발표된 취약점을 이용하여 해킹 수행 코드를 작성할 수 있는 경우
Expert
No
해킹 수행 코드를 수정하여 사용할 수 있는가?
Yes
Guru
발표된 해킹 수행 코드를 수정하여 해킹에 성공할 수 있는 경우
Experienced Technician
발표된 해킹 수행 코드를 수정하더라도 해킹 성공률이 매우 낮은 경우
Technician
No
Script Kiddie
발표된 해킹 수행 코드를 수정 없이 그대로 사용하는 경우
Scripter
각종 해킹 프로그램 및 단순한 Unix 시스템 명령을 사용할 수 있는 경우
Newbie
GUI 형태의 해킹 프로그램을 단순히 사용하는 경우
Kids

- 기존의 일반적인 해킹 기법 분류
  - 사용자 도용(Impersonation)
  - S/W 보안오류(S/W Vulnerability)
  - 버퍼 오버플로 취약점(Buffer Overflow)
  - 구성설정오류(Configuration Vulnerability)
  - 악성프로그램(Malicious Codes)
  - 프로토콜취약점(Protocol Infrastructure Error)
  - 서비스거부공격(Denial of Service Attack)
  - E-mail 관련 공격(E-mail Vulnerability)
  - 취약점정보수집(Vulnerabilities Probing)
  - 사회공학(Social Engineering)

시스템 접근 방식에 따른 공격 분류

- Operating System attacks
  - 공격자는 네트워크를 통하여 접근하기 위하여 운영체제 취약성을 찾고 공격 코드를 활용하여 공격
- Application-level attacks
  - 개발자는 어플리케이션의 많은 기능을 빡빡한 스케줄 내에 개발해야 하므로 다양한 버그가 존재하는데 이를 활용하여 공격
- Shrink Wrap code attacks
  - 운영체제 및 어플리케이션 설치시 관리자가 사용하기 쉽도록 제작된 샘플 코드나 스크립트가 존재하는데, 보안에 취약하므로 이를 이용하여 공격
- Misconfiguration attacks
  - 불필요한 서비스 및 소프트웨어나 잘못 설정된 시스템을 공격