Hacking Process

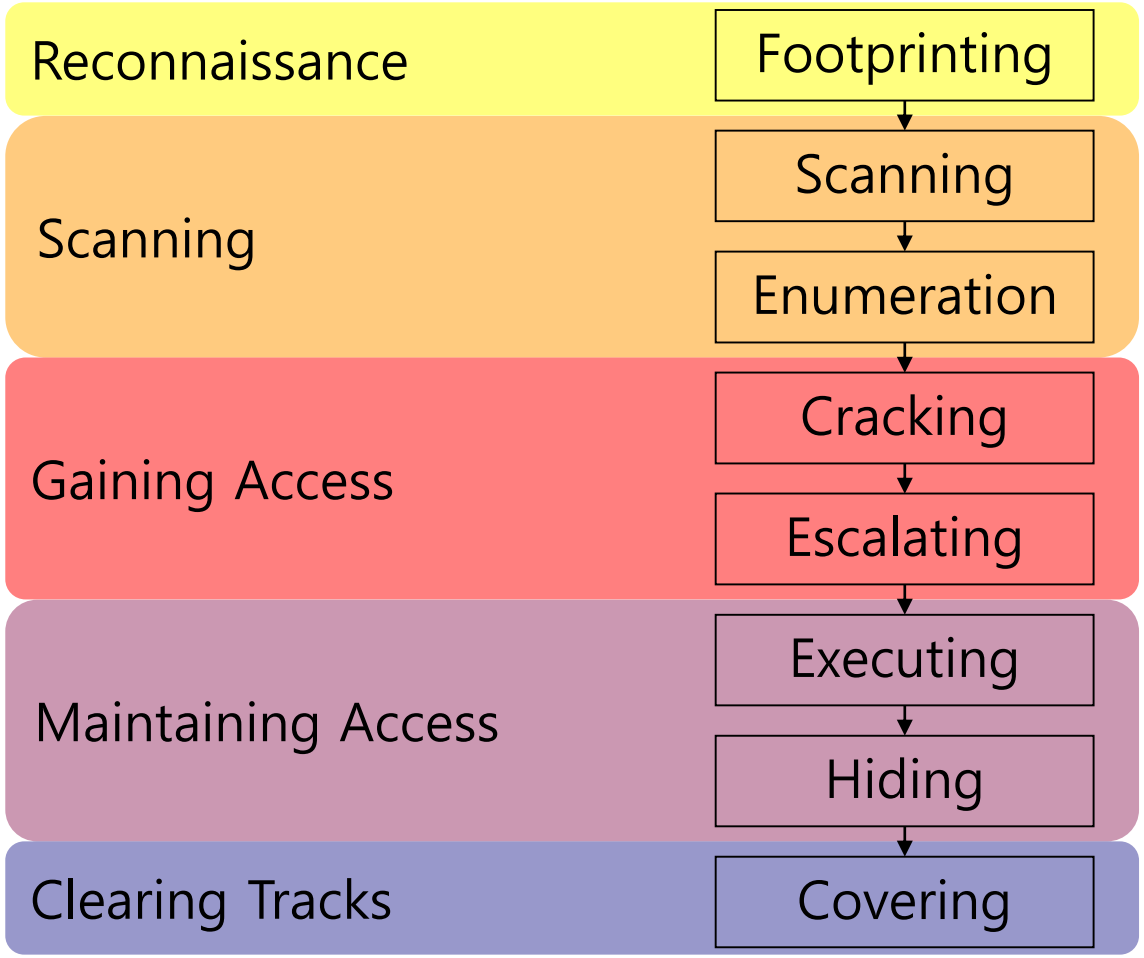
담당교수 : 신원
대상 : 정보보호학과 3/4학년
과목 : 해킹 및 악성코드 대응
학기 : 2020년 1학기

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 많은 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

Hacking Process

Hacking Process Detailed



- 정의
  - Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack
- 세부 활동
  - Footprinting : 공격을 시도할 대상에 대한 정보를 수집하는 작업
- 수집 정보
  - Domain Name, Network blocks, IP addresses of reachable systems, TCP and UDP services r unning, System architecture, ACLs, IDSes running, System enumeration (user and group na mes, system banners, routing tables, and SNMP info)
- 사용 도구
  - http://www.archive.org/
  - Google search
  - whois, nslookup, traceroute/tracert

- 정의
  - Scanning refers to the pre-attack phase when the hacker scans the network for specific information on the basis of information gathered during reconnaissance
- 세부 활동
  - Scanning
    - Include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, and so on
  - Enumeration
    - Extract user names, machine names, network resources, shares, and services

- **정의**
  - 공격을 시도할 표적들에 대한 제공 서비스 및 세부 정보를 확인하는 작업
- **수집 정보**
  - Specific IP addresses, Operating Systems, System architecture, Services running on each computer
- **사용 도구**
  - ping / hping / fping
  - superscan
  - Nmap – TCP / UDP / ICMP scanning
  - ISS Security Scanner, Nessus

- 정의
  - 수집된 정보를 기반으로 유효 사용자 계정 수집 및 취약한 시스템의 공유 자원을 정리&수집
- 수집 정보
  - Network resources and shares, Users and groups, Applications and banners, Auditing settings
- 사용 도구
  - Netbios Null Sessions
  - net use/view , nbstat
  - superscan
  - PS Tools
  - SNScan

- 정의
  - Gaining access refers to the penetration phase. The hacker exploits the vulnerability in the system
- 세부 활동
  - Cracking passwords
    - Crack the passwords of the user and gain access to the system
  - Escalating privileges
    - Escalate to the level of the administrator

- 정의
  - 도구를 사용하여 패스워드로 보안화 한 네트워크 및 시스템 자원에 접근 또는 침입
- 활용 정보
  - passwords
- 사용 도구
  - password sniffing
  - smbcrack2
  - L0phtcrack, ophcrack2, John the ripper
  - pwdump2, pwdump3

- **정의**
  - 시스템 접근 권한을 높여 시스템 관리자의 접근 권한을 획득하는 과정
- **활용 정보**
  - 관리자 정보
- **사용 도구**
  - L0phtcrack
  - Tool : x.exe

- 정의
  - Maintaining access refers to the phase when the hacker tries to retain his/her ownership of the system
- 세부 활동
  - Executing applications
    - Plant keyloggers, spywares, and rootkits on the system
  - Hiding files
    - Use special programs to hide hacking tools and source code

- 정의
  - Plant keyloggers, spywares, and rootkits on the system
- 활용 정보
  - process, keystroke 등 개인정보
- 사용 도구
  - Alchemy Remote Executor, Emsa FlexInfo Pro
  - Handy Key Logger, Ardamax Keylogger
  - Spyware

- 정의
  - The hacker requires root access to the system by installing a virus, Trojan horse program, or rootkit, in order to exploit it
- 활용 정보
  - process, file, registry
- 사용 도구
  - fu
  - AFX Rootkit / Nuclear Rootkit

Clearing Tracks

- 정의
  - Clearing Tracks refer to the activities that the hacker does to hide his misdeeds
- 세부 활동
  - Covering tracks
    - 공격 대상에 대한 모든 접근 권한 획득 후 침입에 관련한 정보 및 도구를 숨기는 과정
- 활용 정보
  - Event log / audit
- 사용 도구
  - auditpol / elsave
  - Winzapper / Evidence Eliminator
  - Traceless / Tracks Eraser Pro