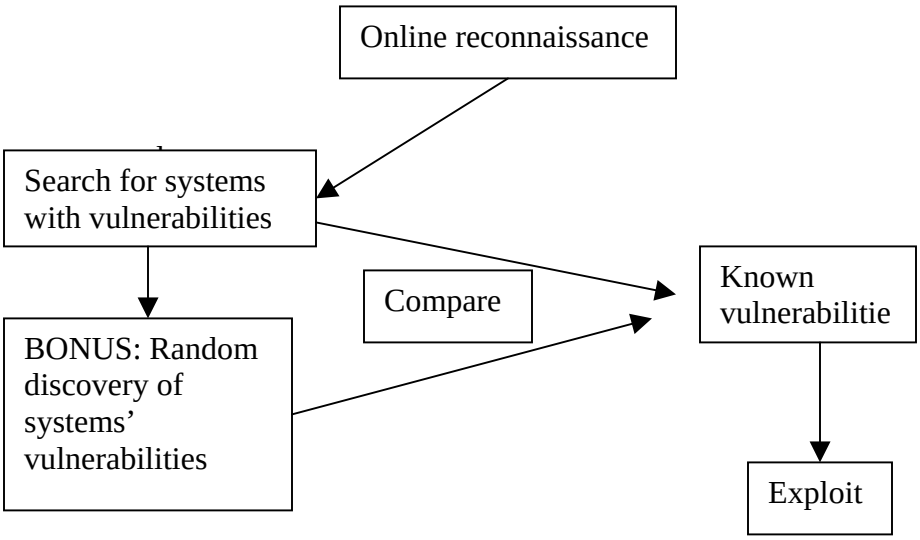
How a Search Engine Can Be Used as a Reconnaissance Tool by a Potential Attacker

Anton Ljutic
Communications Security Establishment

Abstract

1. Abstract Information Technology (IT) systems are increasingly subject to attacks. Most attackers have little knowledge or experience of IT and rely on ready-made applications.
2. An attack on an IT system typically consists of three phases: reconnaissance, penetration and exploit. It is has been said that "no time spent on reconnaissance is ever wasted". During this phase, the attacker collects basic information about the system that is vital to the success of the attack.
3. One method of gathering information is online reconnaissance. There are two approaches to online reconnaissance: direct and indirect
    a. The *direct* method scans networks to directly test the potential victim's vulnerabilities, such as open ports. This method can be very "noisy" and may lead to the victim's increased alertness or even to the tracing of the attacker.
    b. The *indirect* method uses proxies, such as the Google search engine, to noiselessly accomplish some of the objectives of the direct method.
4. Using the Google for online reconnaissance is the subject of the following brief. This method can yield information about a specific site, which can be compared against known vulnerability information. The following examples are given:
    a. Web server version discovery
    b. Web server default installation pages discovery
    c. Site Common Gateway Interface (CGI) script vulnerabilities
    d. Unintentionally exposed directories
    e. Unintentionally exposed files, including sensitive information, ready for download
    f. Other
5. The *purpose* of the brief is to:
    a. Raise the awareness of the threats posed by the existence of sophisticated search engines
    b. Provide practical safeguards to protect against those threats
    c. Demonstrate the advanced uses of a search engine.


Online reconnaissance
Search for systems with vulnerabilities
Compare
Known vulnerabilitie
BONUS: Random discovery of systems' vulnerabilities
Exploit