Lab 10.1: Information Leakage
IN618 Security

May 4, 2015

Introduction

In the processes of carrying out their normal functions it is inevitable that our systems will expose some information about the software they are running. Sometimes this is necessary and sometimes it can't be avoided. But this inforamtion may be of use to attackers, so it's important that we make deliberate choices about what information we seek to disclose.

In this lab we will see two ways that we can gather information about software that is running on a server.

1 Inspecting web headers

We know that web servers send response headers in addition to their payloads with each response. These headers typically contain information about the web server software being used. We can inspect these headers using the text-based `lynx` browser. Log onto `sec-student.sqrawler.com` and run these commands:

```
lynx --head http://www.op.ac.nz

lynx --head http://www.otago.ac.nz
```

By inspecting the headers, and perhaps by searching the web a bit, answer the following questions about each we server:

1. What kind of web server is the site running?
2. What other software or services are used to deliver the site?

We get a limited amount of information from this method and we can't even be sure that it's accurate. But we may still learn something that will help us plan an attack. Since we're just making routine web requests, there's nothing about our actions so far that warn system operators of a possible attack.

2 Port scanning

There are other scanning methods that can gather more information. *Port scanning* is one such technique. Although it gathers more and better information for an attacker, port scans can be detected by system operators and should be regarded as the first stage of an intrusion attempt. **Do not perform invasive port scans of systems without the consent of their operators. In some cases you may be liable for criminal prosecution.**

For this lab you may perform scans of the systems set up for this exercise. The lecturer will indicate the IP addresses of servers you may scan. You will also be given the address of a system that you will `ssh` into to perform these scans.

```
nmap -sv --version-light <target ip address>

nmap -sv --version-all <target ip address>
```

The first scan is quicker but yields less information. The second scan takes a long time and produces a more thourough report. Scan one or two of the sample addresses and note your findings below.