# What’s your friend doing?

Final report for Introduction to Computer Security

車曉宇

Computer Science of National Chiao Tung University

Email: [chexiaoyufrank@gmail.com](mailto:chexiaoyufrank@gmail.com) Student No:0340299

Abstract

With the development of the Internet, the technology of hacking is developing rapidly. As long as we surfing on the Internet, we are in the danger of being hacked, in another word, we are exposed on the Internet. The course of “Introduction to Computer security” is funny and useful, which make me more interested in computer security and network security. Thanks for this course, I get touch with lots of theories and tools about computer security, and I understand the importance of protecting the equipment from hacking.

Technology is a double-edged sword. It is kind or evil depending on how we use it, so as hacking technology. It’s a truth that any system may have vulnerabilities or loopholes, but it doesn’t mean that we should exploit vulnerabilities to do something bad. Maybe we only want to play a joke on the client users. And the target of this course would not be providing us some skills to do bad things, but protecting equipment from attacking.

The behaviors of mine in the report are aiming to play a joke on my friends who are surfing on the Internet. What I want is to get the information of his behaviors.

Tools

Nmap

Nmap (Network Mapper) is a security [scanner](https://en.wikipedia.org/wiki/Network_scanner) originally written by [Gordon Lyon](https://en.wikipedia.org/wiki/Gordon_Lyon) (also known by his pseudonym Fyodor Vaskovich) used to discover [hosts](https://en.wikipedia.org/wiki/Host_(network)) and [services](https://en.wikipedia.org/wiki/Web_service) on a [computer network](https://en.wikipedia.org/wiki/Computer_network), thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted [packets](https://en.wikipedia.org/wiki/Network_packet) to the target host and then analyzes the responses.

The software provides a number of features for probing computer networks, including host discovery and service and [operating system](https://en.wikipedia.org/wiki/Operating_system) detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including [latency](https://en.wikipedia.org/wiki/Network_latency) and [congestion](https://en.wikipedia.org/wiki/Network_congestion) during a scan. Nmap is under development and refinement by its user [community](https://en.wikipedia.org/wiki/Community).

Nmap was originally a [Linux](https://en.wikipedia.org/wiki/Linux)-only utility, but it was ported to [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), [Solaris](https://en.wikipedia.org/wiki/Solaris_Operating_System), [HP-UX](https://en.wikipedia.org/wiki/HP-UX), [BSD](https://en.wikipedia.org/wiki/BSD)variants (including [Mac OS X](https://en.wikipedia.org/wiki/Mac_OS_X)), [AmigaOS](https://en.wikipedia.org/wiki/AmigaOS), and [SGI IRIX](https://en.wikipedia.org/wiki/SGI_IRIX). Linux is the most popular platform, followed closely by Windows.

Reference

1. Nmap-Wikipedia, the free encyclopedia, <https://en.wikipedia.org/wiki/Nmap>.