Introduction to Cyber Security

We use computers for everything from space investigation to shopping and communicating with friends through email or chat programs. Although you may not consider your communications much of a high confidential issue, you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer.

Intruders may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems. Having control of your computer, gives them the ability to hide their true identity as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have, a computer connected to the Internet only to play games or to send emails to friends and family, your computer may be a target.

One of the many techniques used to compromise your computer by the attackers is Operating System Fingerprinting. Operating System (OS) fingerprinting is the process of learning what operating system is running on a target device.

According to Wikipedia,

"TCP/IP stack fingerprinting (or OS fingerprinting) is the process in computing of determining the identity of a remote host's operating system by analyzing packets from that host."

Why OS Fingerprinting?

When an attacker is trying to hack into any computer, he starts to gather information about the computer (target) as much as possible. Major Key information is the operating system the target is running on. As long as this information is not revealed, the attacker is limited in the variety of attacks, probes and exploits. Therefore the focus on initial information gathering is finding out the operating system.

There are several approaches to finding out the running operating system of an unknown host without having an account or any other way of logging in directly on this machine. Some of the many OS Fingerprinting techniques are;

1. Direct Banner Grabbing (Classical Fingerprinting)
2. Active IP Packet Fingerprinting
3. Passive IP Packet Fingerprinting

Classical Fingerprinting

Even without using any automated techniques of any kind, hosts will often announce their OS to anyone making a connection to them through welcome banners or header information. For example, when connecting to a host via the standard Telnet protocol the OS version is often sent to the client as part of a welcome message.

Example from "Techniques in OS-Fingerprinting" by Nostromo:

In UNIX like platforms, when using Telnet Protocol;

```
root@nostromo# telnet mail.fh-hagenberg.at 143
Trying 193.170.124.96...
Connected to postman.fh-hagenberg.at.
Escape character is '^]'.
* OK Microsoft Exchange Server 2003 IMAP4rev1 server
version
6.5.7226.0 (postman.fhs-hagenberg.ac.at) ready.
```

When analyzing the output a lot of information is revealed from the single line that was returned by the server. Now it is up to an attacker to find an exploit for this specific version of the Microsoft Exchange Server 2003.

Active IP Packet Fingerprinting

Active operating system fingerprinting is the method of actively determining a targeted network node's underlying operating system by probing the targeted system with several packets and investigating the response. The traditional approach is to examine the TCP/IP stack behavior (IP, TCP, UDP, and ICMP protocols) of a targeted network element when probed with several legitimate packets.

We can automate this technique using "nmap" software tool.

According to "Techniques in OS-Fingerprinting" published by Nostromo;

"nmap begins its OS detection by sending an ICMP ping request to the target. Then it connects to port 80 (HTTP) to see if the target is responding and running at all. Then nmap does the actual portscan, searching for at least one open (an application listening and waiting for connections) and one closed (no application is listening on this specific port) port. To gain exact information about the underlying OS nmap sends several special crafted TCP packets and

records the replies. It then makes a lookup in the OS-detection fingerprint file and detects the Operating System which the target is running on."

Passive IP Packet Fingerprinting

Passive fingerprinting is based on sniffer traces from the remote system. Instead of actively querying the remote system, all it needs to do is capture packets sent from the remote system. Based on the sniffer traces of these packets, you can determine the operating system of the remote host. Just like in active fingerprinting, passive fingerprinting is based on the principle that every operating system's IP stack has its own individual characteristic. By analyzing sniffer traces and identifying these differences, you may be able determine the operating system of the remote host.

"Ettercap" is a package that is available for most common operating systems (Windows, Mac OS X, Linux, and FreeBSD) which collects and dissects packets from a network.

According to Ettercap official web site:

"Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis. "

Avoiding Fingerprinting

"Every problem has a solution" this saying is true for our context, which is OS fingerprinting. There is always a risk of someone steeling your OS information, in the same time there is a mechanism of overcoming this problem. There are number of ways that we can avoid OS fingerprinting.

It is so easy to avoid classical fingerprinting (Daemon banner grabbing). Daemon banner grabbing happens through the welcome massage that applications use to send when starting a conversation. This problem can be solved by simple editing the welcome massage. In the same time, we can edit that in such a way that attacker get the wrong information and that information mislead him. Another technique is to provide the attacker with a long daemon banner and in the mean time track him.

This problem can also be solved by use of a firewall. Many firewall products now provide this functionality out of the box. Firewall software provides a language that allows responses to be crafted to particular packets, thus actively spoofing the target OS.

In the Sri Lankan context it is harder to do a (active) OS fingerprinting, as most of Sri Lankan systems using a NAT (Network Address translation) system, even though we use NAT as a system to overcome the limitation of IPv4 addresses this can be use as a security technique. When we are using NAT outsider do not have the direct access to our machine. In this scenario, the host's network is typically given a 'private' network designation (10.0.0.0, or 192.168.0.0). An intelligent gateway accepts outgoing packets from hosts do the address translation, which will assign that packet a global IP and a new port. Upon return, the gateway transparently reinstates the original address and forwards the packet to the original host. This effectively makes all traffic to or from the network appears to be coming from the one node, making identification of hosts on the private network very difficult.

Always we have to keep updated with the technology, when there is a exploit in a OS, the manufacture tend to develop a patch to overcome that, so uses need to install them as soon as possible.

EX from "Techniques in OS-Fingerprinting" published by Nostromo:

"IP Personality1 is a patch for Linux kernels of version 2.4, which modifies the characteristics of network traffic. Things that can be influenced are the TCP Initial Sequence Number, the TCP initial window size, the TCP options (their types, values and order in the packet), the IP ID numbers and answers to some pathological TCP packets. After applying this patch iptables has new targets that can be used in the mangle table. "

The future of OS Fingerprinting

A current focus of software development houses is one of computer security, with Microsoft launching its "Trustworthy Computing Initiative" (According to Trustworthy Computing Initiative", Microsoft website) and many OS vendors initiating an automated patch download/update service. Examples include Microsoft's Windows Automatic Update service included in Windows 2000 and onwards, and the Redhat Network service available via the up2date utility in Redhat Linux. These developments, coupled with the general improvement in the world's cyber laws and prosecution rates, are slowly 'raising the bar' on cyber attacks. In this climate, general 'script kiddy' mass-scans may prove too dangerous or fruitless to pursue.

According to "An Overview of Remote Operating System Fingerprinting" by SANS Institute InfoSec Reading Room, "The attacks of the future may be well directed and customized according to OS and services running on the target. This may be considered normal worm activity in the future."

Conclusion

OS fingerprinting is a fascinating subject that is of interest to the security community. There are lot of techniques to do OS fingerprinting in the same time there are number of ways to overcome/avoid OS finger printing. Remote OS Fingerprinting is a recent development on the Internet and one to watch. The ability to remotely determine, with high accuracy, the Operating System of a remote host on the Internet is a powerful one. Even though it is limited to a certain part of users due to the lack of global IP addresses, this will rise with the new IPv6 addresses. In future, there will be extremely customized new attacks that will overcome all the barriers and will be harder to avoid. The general trend towards increasing penalties for being caught as the world's cyber laws improve may also serve as a driver towards more refined attacks in the future.

What we have to remember is that, this is like a race when hackers come up with a solution to avoid OS fingerprinting crackers come up with a counter technique; hackers again develop a counter-counter technique that will avoid the new technique discovered by crackers. This cycle never ends. All what we have to do is getting updated with the most recent technology to deal this.

Reference

[1] Wikipedia Encyclopedia "http://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting/"

[2] "Techniques in OS-Fingerprinting" published by Nostromo, Hagenberg, September 2005

[3] Ettercap Official web site "http://ettercap.sourceforge.net/"

[4] Netmap Official web site "http://www.netmap.com.au/"