Counter-measures for operating system fingerprinting

by Riaan Stopforth, Luke Vorster and Dr. David Erwin, University of KwaZulu-Natal

The first step in the methodology of attacking a system on a network is by port scanning and operating system (OS) fingerprinting. An investigation was undertaken to determine if this can be prevented, by discouraging the attacker from continuing the attack of the unknown system and so preventing further steps from being taken. This was performed by using OSF and focusing on an OS such as Linux.

The prevention of port scanning is impossible, to a certain degree, as many systems have open ports, especially the web servers and systems that are commonly known to have open ports. Countermeasures for OS fingerprinting is the next necessary step. It is important for the attacker to know what OS is running on the target system, as each OS has different vulnerabilities. The attacker might have one opportunity to penetrate the target system, before the system either notifies the network administrator that an attack is happening, or it enters a denial of service (DoS) mode.

A number of OS fingerprinting tools were investigated, and it was found that the two best scanners were Network Mapper (Nmap), by Fyodor (www.insecure.org/nmap) and Xprobe2 by Ofir Ahin (www.kvz.org/linux). To a certain extent these tools work differently to obtain a fingerprint from an OS.

The OS fingerprint is determined by the values of the fields in the TCP/IP stack. The headers of the TCP and IP are seen in Fig. 1 [1] and Fig. 2 [2] respectively. Different formats of packets are sent to the target system, and depending on the reply of the target system as well as the values of the fields in the TCP/IP stack, the OS can be uniquely identified. Some versions of OS cannot be differentiated as the developers have not altered the fields in the TCP/IP stack, which is often needed should this cause a vulnerability.

There are tools available that allow the alteration of the fields in the TCP/IP stack. These alterations can also be done by modifying the kernel configurations. This option is not recommended as a countermeasure, as these alterations of the fields in the TCP/IP stack can cause the performance of communication across the network to be of sub-optimal value.

The advantage that Xprobe2 has over Nmap is that it uses the internet control message protocol (ICMP) which is seldom blocked by firewalls. The observation was made that Xprobe2 was easily deceived when the TCP/IP stack was altered, or when ICMP messages were blocked at the firewall. Nmap on the other hand was still able to identify the OS with these modifications. This is as a result of Nmap’s large database. The database consists of 1681 different fingerprints, and most of them are duplicates of an OS with alterations for the different fields.

Research indicated that the best way to counteract the OS fingerprinting from attackers is to use the same techniques that they are using.

Evgeniy Polyakov used this technique to create a module for IPtables called OSF. OSF can be found at http://tservice.net.ru/~sombre/archive/osf/. This module was specifically designed to allow communication between systems running on a specific OS. Incorporating this technique, Nmap has its unique fingerprint. With the use of IPtables, the system could drop all packets that are identified as Nmap scan packets. There are a couple of improvements that could be applied to the OSF module, but its benefit at this stage is that other scanner’s fingerprints can be added to OSF’s database, thereby blocking any scans from them as well. Furthermore, OSF has the option to log these scanning attempts.

For Nmap to perform accurately, it needs to find an open and a closed port on a system. With the installation of OSF on a target system, it is not possible for Nmap to fingerprint the OS on it as OSF also drops all packets that Nmap uses for port scanning.

There are other suggestions for countermeasures of OS fingerprinting that need to be taken into account. Tools are available that monitor the response of a system when the attacker attempts to connect to port 0 of the target system. Therefore the suggestion is that all packets sent to this port are dropped.

Some OSes such as Linux have the type of service (TOS) field set to 0xC0. When the system acts as a router, the value of the TOS field is set to 0xC0. The OS of a system can be fingerprinted if its TOS field is 0xC0 and it is not a router. It is suggested that the TOS field is set to 0x00 for all packets.

 Lastly, the suggestion is that all ICMP packets be dropped. ICMP packets are used to help with the communication across the network, but communication is still possible without them.

Conclusion

Securing a network or system is a challenge, especially with new vulnerabilities that are discovered daily. Some of these countermeasures could discourage an attacker, but not necessarily prevent the continuity of the attack. A determined attacker could successfully penetrate the system. It is suggested that the system administrators check for new vulnerabilities, and use the latest patches to update the systems. The checking of log files is important. If any unusual activities are found, or a scan is detected, then further investigation is needed to determine if similar packets from the IP address of the attacker should be dropped.

References


Contact Riaan Stopforth, Tel 072 255 3330, stopforth@ukzn.ac.za