Maluki Muthusi
P15/81741/2017

An Evening with Berferd

Bill Cheswick was able to lure a cracker into believing he had succeeded in exploiting the sendmail DEBUG hole in the AT&T system, (Cheswick 1992). The cracker was using other machines, which he had hacked to launch his attacks.

The cracker try to use well vulnerabilities that were running on the system. Some of these programs were ftp, telnet, smtp and rsh. The attacker also tried to delete all the files in the system in cover his tracks.

Cheswick contacted the Stanford team since the attack had came from one of their computers. Standfor reported the account used was a stolen. During this time Cheswick and his team did set up a jail system. A system that is a clone of the production system but dangerous commands removed. Commands such as ps, which would let the attacker view all the processes on the system.

Berferd was traced and linked to be Dutch hacker. They were unable to prosecute them because hacking was not illegal under Dutch law at the time. Berferd was patient and had a pool of machines which he could launch his attacks from.

The story of Berferd shows how data protection laws must be implemented in all the countries to avoid providing bases for hackers.

References

Cheswick, B. (1992), An evening with berferd in which a cracker is lured, endured, and studied, *in* 'In Proc. Winter USENIX Conference', pp. 163–174.