Contractor Performs Unauthorized Security Scans

Case Study

You have been called as an expert witness in a criminal trial in which the defendant has been accused of performing unauthorized security scans on a large corporation. Your task is to determine whether or not the defendant's actions are consistent with criminal intent.

Case narrative

A prosecuting attorney has recently hired you as a consultant to provide expert testimony in an upcoming criminal case. The case focuses on a technical contractor who was recently fired for performing unauthorized penetration testing on the employer's computer systems. After reviewing the facts with the employer, the prosecutor is considering bringing criminal charges against the worker.

The employer is a manufacturer of mobile and embedded computing systems, with products that include custom circuit boards, custom processors, and consumer electronics. The company had recently expanded its consumer focus to produce a new smart phone. The contractor, who had been with various divisions in the company for the previous two years, was hired by the smart phone division to advise on the security features of the phone, as well as best practices for protecting the intellectual property related to the phone's design.

Three months after the contractor began working with the smart phone division, a system administrator in the custom processor division discovered unauthorized processes started by the contractor. These processes included password cracking tools, network port scans, and a scanner for privilege escalation vulnerabilities. The system administrator stated that these tools are commonly used during initial reconnaissance as steps toward a security breach. The computers targeted by these tools stored propietary processor designs, including some intended for sensitive government contracts. As this work was unauthorized, the contractor was immediately fired.

The lawyer has sought your advice to determine if the following two criminal charges are appropriate. These charges would be classified as felonies under state law:

- Altering without authorization two computer systems.
- Accessing a computer with intent to commit theft.

Historical context and additional discussion

Randal Schwartz, a well-known figure in the open source community and author of several popular Perl books, worked as a contractor for Intel from 1988 to 1993. His consultant duties included security consulting. In late 1993, he ran a password cracking tool on a machine operated by Supercomputer System Division (SSD), the successor of his former division. Finding a weak password, he continued to investigate and used the tool on other SSD machines and their main server cluster. However, as Schwartz's contract at the time did not include monitoring SSD systems, these scans were considered unauthorized. Schwartz was convicted of three Computer Crime felonies under Oregon law. His convictions were expunged in 2007.