

Kevin Berry

Application Layer and Network Security

I want to investigate network security. Specifically, I want to cover mostly application layer security, but I will also go over network layer security like TCP/IP. The application layer protocols I want to go over will be encryption and cryptographic protocols such as SSH and SSL. I will also investigate vulnerabilities in certificates such as SSL and public key cryptography, and ways people can circumvent them if they're not properly implemented by programmers. Also, I want to go over some popular cryptographic methods like Md5 and Sha-1, which are used to encrypt passwords for data validation. Recently, they have been semi-hacked. I will show how to fake an CRC like one of the above and the availability of rainbow tables to find matching keys for data.

There are a couple of pieces of open source software, such as Tripwire and nMap, which help network administrators keep out perpetrators. These types of software test all sorts of vulnerabilities on networks.