Shorebreak Security, 8635 Holiday Springs Road, Melbourne FL 32940,
info@shorebreaksecurity.com

Case Studies in Penetration Testing

Background

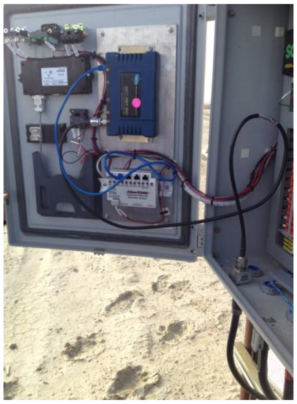
In our experience, successful penetration tests rely heavily on manual testing. The skills and abilities brought to the table by an experienced penetration test team emulate those of the threat – the criminal hacker. While Automated Vulnerability Scanners and Exploitation Frameworks do have a place, they are severely limited by the signatures or modules contained in the tool and no one should rely on them to detect all vulnerabilities.

The following are a few examples of penetration tests conducted by Shorebreak Security and illustrate why there is currently is no replacement for a good, human tester.

Wolves are Guarding Your network

Penetration testing may often include the exploitation of physical access controls to network components and computers.

On one assessment, Shorebreak Security found that the customer, a global gas and oil company was communicating with remote well installations using radio communications.



Internal access to the company's network could be gained by simply driving into a remote area of the wilderness, opening an unlocked utility box, and plugging a laptop into the network port readily available there. This gave the test team direct access to the SCADA network.

Once on an internal network, attacks become much easier since internal network components are almost always less secure than the external boundary.

Instituting an Open Door Policy at a Large U.S. City

During an assessment for a large U.S. City, the Shorebreak Penetration test team found that connecting to the Wi-Fi network in the local public library yielded access to the city's entire internal network. Again, once the team is able to access the internal network, workstations, servers and other components become easy targets for exploitation.

In this particular case, however, the impact was far more critical because the devices reachable on this network included the local CCTV system as well as building access control server that controlled access to the police gun vault, evidence locker, narcotics vault and holding cells, along with countless other important doors in the city complex. Shorebreak Security engineers could simply right click on a door and disable the HID card reader and enter at will.

Someone is testing your network right now. You should be too.

These are just two examples of the many penetration tests across government and commercial industries performed by Shorebreak over the last years. Each test is different and presents its own set of unique challenges. Having humans manually test the systems and trying to outsmart the security mechanisms has almost always led to the discovery of critical vulnerabilities.

About Shorebreak Security

We are a veteran-owned small business providing exceptionally high-quality, high-value Information Security consulting services.

We specialize in conducting a variety of relevant, real-world Information Security tests that show you where your weaknesses are. We translate Information Technology risk into organizational risk, and empower you to make informed decisions

Contact Us:

Shorebreak Security, 8635 Holiday Springs Road, Melbourne FL 32940
info@shorebreaksecurity.com - 1-888-838-7311