UC-12 Simulated Small Business Security Program

INTRO/ABSTRACT

The goal of our capstone project was to develop a secure e-commerce site for a small online company. To accomplish this goal, we started by developing a business scenario, building an e-commerce server, and creating a comprehensive security program to protect this server. We tested and documented our procedures and created a Risk Assessment and Information Security policy to be used as guidelines for the security of our company.

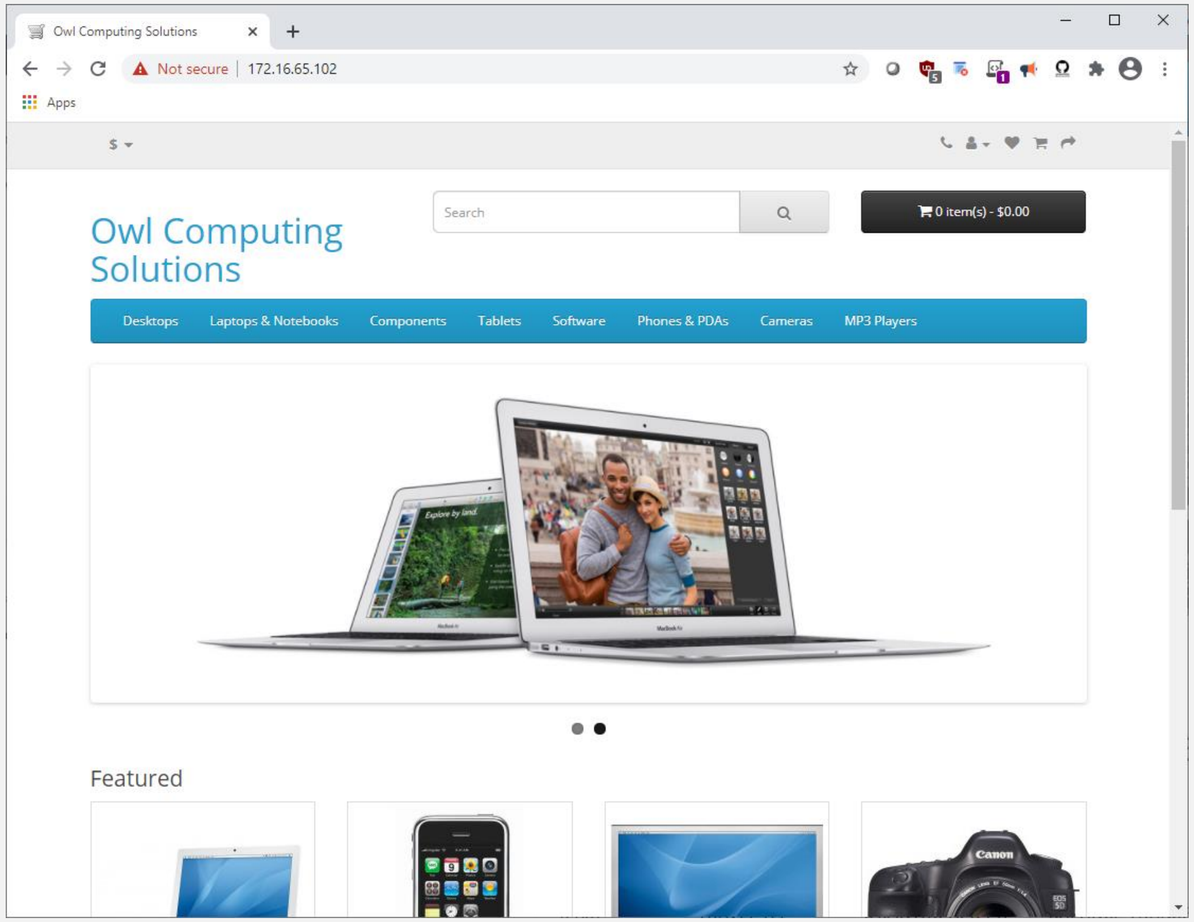
METHODS

We explored various open-source e-commerce, web server, database and security software to determine which packages would be best to provide a great e-commerce experience while keeping our server secure. As a best practice, we tested these platforms and their compatibility offline before implementing them to our production server. For our e-commerce platform, we chose OpenCart running on the Nginx web server. We used the UFW firewall and SSL to protect our server and we used a combination of Snort and Nagios for intrusion detection and network monitoring.

RESULTS

After our server was complete, we were asked to attempt to exploit servers belonging to other capstone teams. We were able to successfully infiltrate all the other servers from both a command line and database level.

Create an e-commerce site together with a comprehensive security plan for our team's company, "Owl Computing Solutions".



Our Team Site contains additional information about our project and our team.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s) - Hristo Bakalov, Watson Day, Patrick McCollums, Philinda Morse, Tyler Phillips
Advisors(s) - Dr. Ying Xie, Dr. Lei Li