CIS399

Team Ninjas

8/15/17

Final Project Proposal

Goals:

* Build and configure XMPP OpenFire server for IMing/messaging
* Install and configure MySQL to use as embedded database for OpenFire
* Verify that IMing/messaging capabilities work from a client machine
* Install and configure Fail2Ban to prevent network attacks
* Automate Fail2Ban installation and configuration via Puppet

Testing Methods:

* Install Pidgin chat client on a client machine and verify that chat client can connect to XMPP server
* Verify that two users can send and receive chat messages from one another when connected to XMPP server using Pidgin chat client
* Verify that Fail2Ban automatically installs on all puppet agents using puppet modules
* Verify that Fail2Ban rules can be automatically pushed to agents by checking agents to ensure that rules are being populated from puppet master

User Impact:

* Gives users IM/messaging functionality which could improve communication and collaboration abilities
* By virtue of Fail2Ban increasing the overall security and stability of the environment, users will experience less downtime, slowness, or compromises that might otherwise occur due to events such as brute force SSH attacks
* Short of nefarious user intentions, Fail2Ban should not affect or prevent users from using the chat functionality of the XMPP server

Security Issues:

* MySQL has a number of security vulnerabilities that could be mollified by using a strong DB password, running the MySQL DB security script to disable settings such as anonymous logon, and allowing least privileged access to the databases
* Administration of OpenFire is performed over the browser through an “admin console”. Ideally we should be using an SSL cert to access this console.

Steps to Completion of Work:

* Installed Fail2Ban
* Automated installation and configuration of rules via Puppet
* Installed MySQL server on the server
* Created MySQL database, MySQL user account/s, MySQL grants, and imported OpenFire schema
* Installed and configured OpenFire
* Tested connectivity between client and server using Pidgin chat client

Maintenance/Automation:

* To maintain this service we will need to continually ensure OpenFire is kept up to date. Puppet could likely be used to automate updates.
* Continue to use Puppet to automate Fail2Ban rules.
* Ensure Fail2Ban rules are fine-tuned to prevent network attacks on our servers, especially for attacks our servers appear to be extra susceptible to.
* Periodically audit users of our OpenFire/XMPP service

Documentation:

* <https://github.com/cis399-2017-team/Ninjas/tree/master/finalproject/OpenFireConfigurationNotes.txt>
* <https://github.com/cis399-2017-team/Ninjas/tree/master/finalproject/Piden.conf>