The Center for Cyber Defenders

Expanding Computer Security Knowledge

SAND2015-5712C

Emulating Network Isolation Zones

Project Mentor: Paul Sery, 9312

Lance Chao, Virginia Tech; Rain Dartt, Rose-Hulman Institute of Technology;
Russell Van Dam, New Mexico Tech

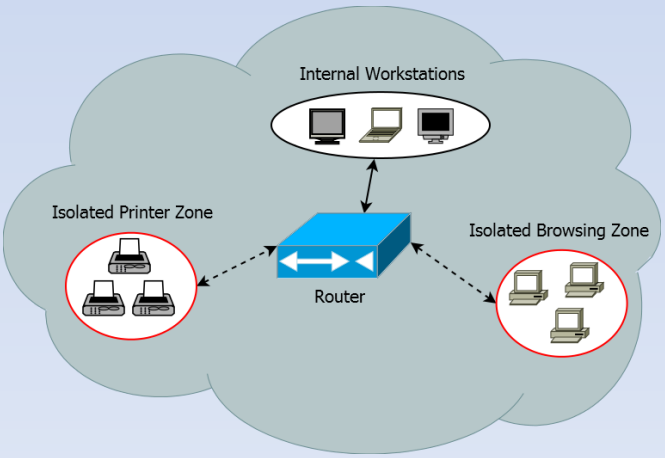
Problem Statement:

Isolation Zones create logical, filtered network segments based on device classes, such as printers, within an existing network. The filters provide only enough access to allow each class to function properly. This architecture organically protects one segment from another by restricting malware attack vectors.

The Isolation Zones concept has been deemed valid, but testing with real machines is difficult. There is currently no practical way to test a variety of large, topologically complex networks containing isolation zones.

Objective and Approach:

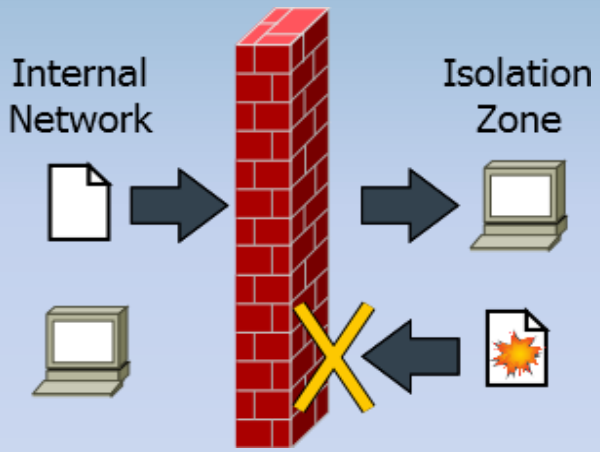
- Create a scalable system of emulated computers configured for a standard enterprise network using Minimega
- Develop ways to section off subnets with different network traffic protocols
- Measure the effectiveness of the isolation zones for each topology



Isolation zones separated within the network

Results:

- Wrote a Minimega script that launches a predefined network topology with preset traffic forwarding rules for each subnet
- Verified network configuration with *nmap* and packet analysis to ensure subnets are properly isolated



Depiction of one-way traffic between subnets

Impact and Benefits:

The testing environment can be used to monitor the spread of malware among subnets with and without the added security of isolation zones. This will provide quantifiable data to support our hypothesis that isolation zones help simplify a large, heterogeneous network into homogeneous subnets. These smaller zones will have reduced network access based on the needs and intended uses of devices in the zone.