SAND2018-7535D

The Center for Cyber Defenders

Expanding computer security knowledge

Moving Target Defense

Nomaan Dossaji & Spencer Schrock, University of Illinois at Urbana-Champaign
Julian Tuminaro, Carnegie Mellon University

Project Mentor: William Stout, Org 9315

Problem Statement

Moving Target Defense (MTD) aims to prevent cyber attacks by dynamically changing aspects of the environment. There are both network and host based MTDs. One host based technique is OS Rotation which utilizes different operating systems that all run an identical service. A single OS is live for a set time interval while other OSes take turns rotating in.

The practicality of OS Rotation has not been researched extensively.

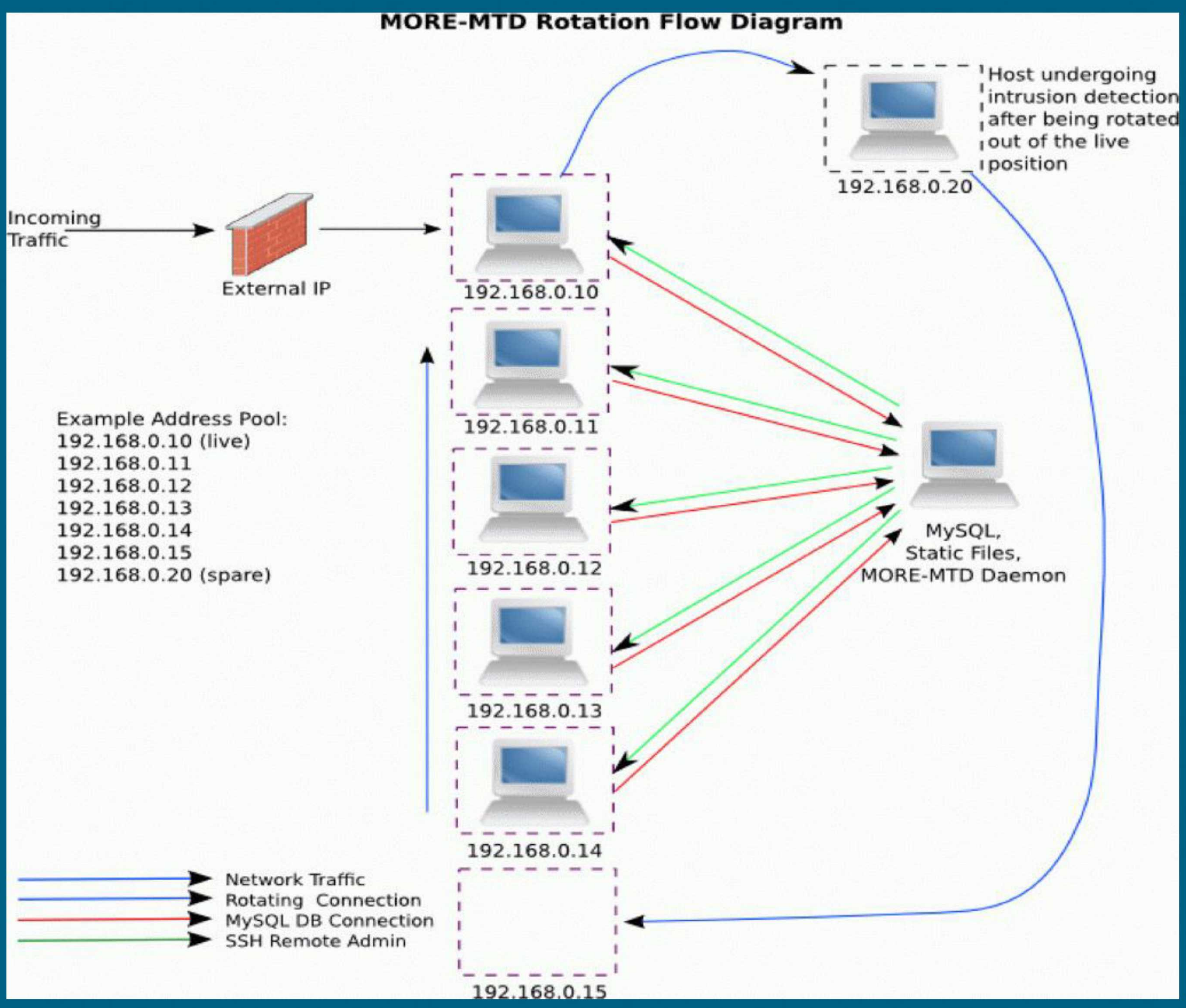
Objectives and Approach

Our goal is to examine various aspects of a running service in an OS Rotation environment:

- Test different time intervals between rotations
- Examine the effectiveness of performing attacks on a vulnerable environment
- Look at possible side effects such as latency, packet loss, and overhead

Impact and Benefits

This project will assess the viability of OS Rotation. With a minimal amount of data obtained at this point, we are speculating that this iteration of OS Rotation has little effectiveness of preventing high threat attacks. Whereas attacks that examine a network for vulnerabilities and exploit these vulnerable systems are less effective against MTD. OS Rotation will not necessarily prevent vulnerabilities, but it will deter attackers that are not knowledgeable regarding the system.



Argonne: MORE MTD - https://coar.risc.anl.gov/research/more-mtd/

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.