SAND2016-7227C

The Center for Cyber Defenders

Expanding computer security knowledge

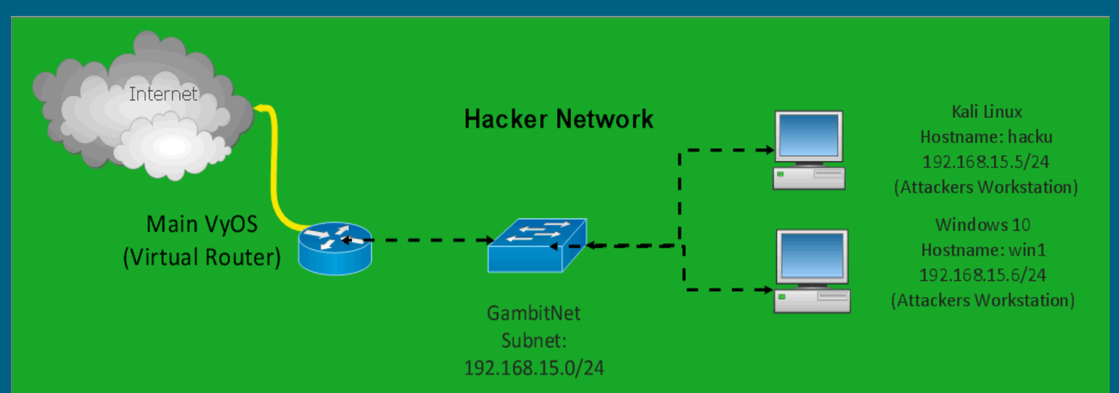
TracerFIRE 7 System Design

Justin Njenga, Bowie State University; Joshua Russ, Voorhees College; Montrey Freeman, Allen University;

Project Mentor: Kim Ta, 9315

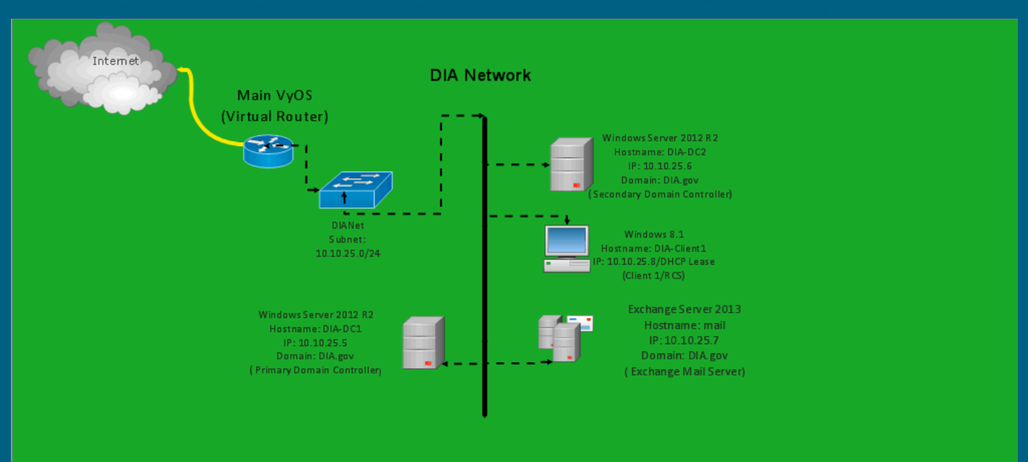
Problem Statement:

- Develop a virtual infrastructure that may be incorporated and used amongst the various teams for the TracerFIRE 7 project.
- The virtual infrastructure must match the premise of the adopted story for the TracerFIRE 7 build. This includes an 'attack' network, a 'victim' network, and a network to bridge multiple networks.
- Designing, modeling, installing, and configuring require a diversity of skills heavily influenced by networking, client/server infrastructure, and operating systems.
- The configuration of the virtual networks must accommodate the forensics team, and the malware team so that they may carry out their respective task that require the network connectivity.



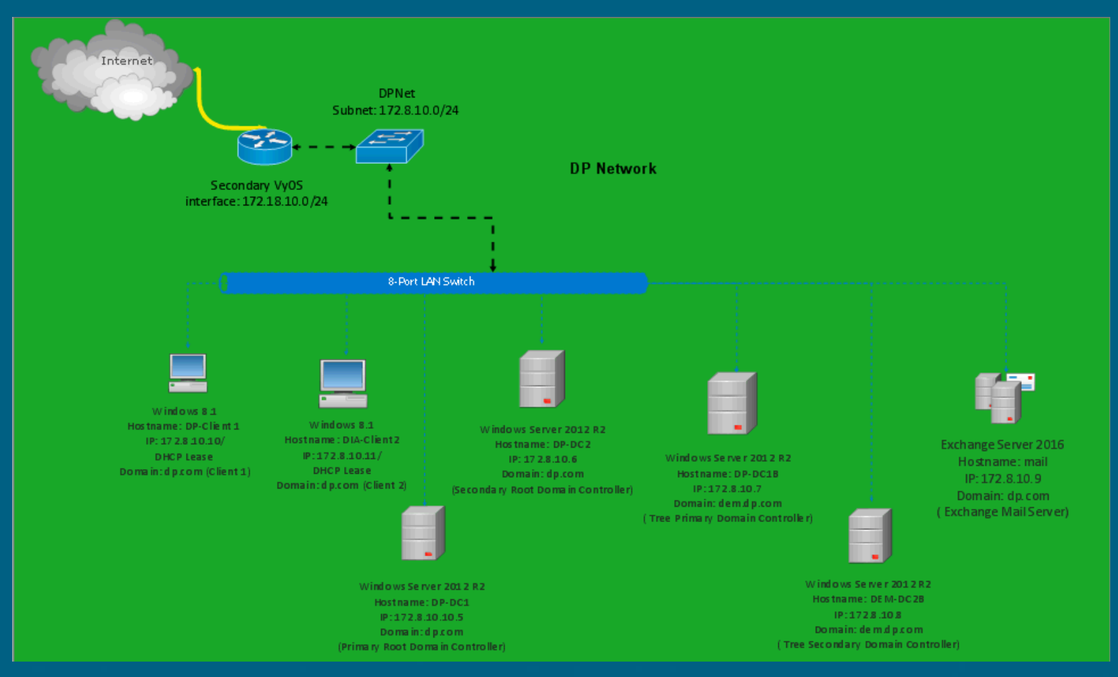
Objective and Approach:

- The Virtual System is designed for the malware team to develop an exploit(s) that will serve as a training module for participants to determine methods of exploiting a system.
- Using the hypervisor Xen Server 7.0, virtual machines are used to replicate an enterprise network that will be incorporated for the TracerFIRE 7 training module.
- Xen Server is installed on a Dell PowerEdge R610 rack server. This server is currently configured with two hardware RAID configurations for data insurance & performance.



Results:

- Configure a functioning virtual network that replicates that of a physical network. This includes separate networks routed by the operating system VyOS. In addition, the virtual network currently allows the virtual machines to communicate as nodes on a network.
- Install, configure, and administer a working windows domain environment. This domain structure includes a plethora of windows domain controllers, windows domain clients, and a working email exchange server. Systems are built across networks which include the following operating systems: Windows Server 2012 R2, Windows 7 , Windows 8.1, Windows 10, and Exchange Server 2013 & 2016 built on Windows Server.
- Diagram to represent the system infrastructure, as well as the network design including but not limited to the networks, domains, and routing handled by VyOS.



Impact and Benefits:

- The development of the virtual system may be used as a training model for network & system administrators on modeling and building a network and a system infrastructure.
- The configuration of the network and system may be used for security experts to analyze possible vulnerabilities that may be exploited.
- Interacting with this virtual system will also train participants on properly hardening system based on vulnerabilities exploited.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-XXXXC.

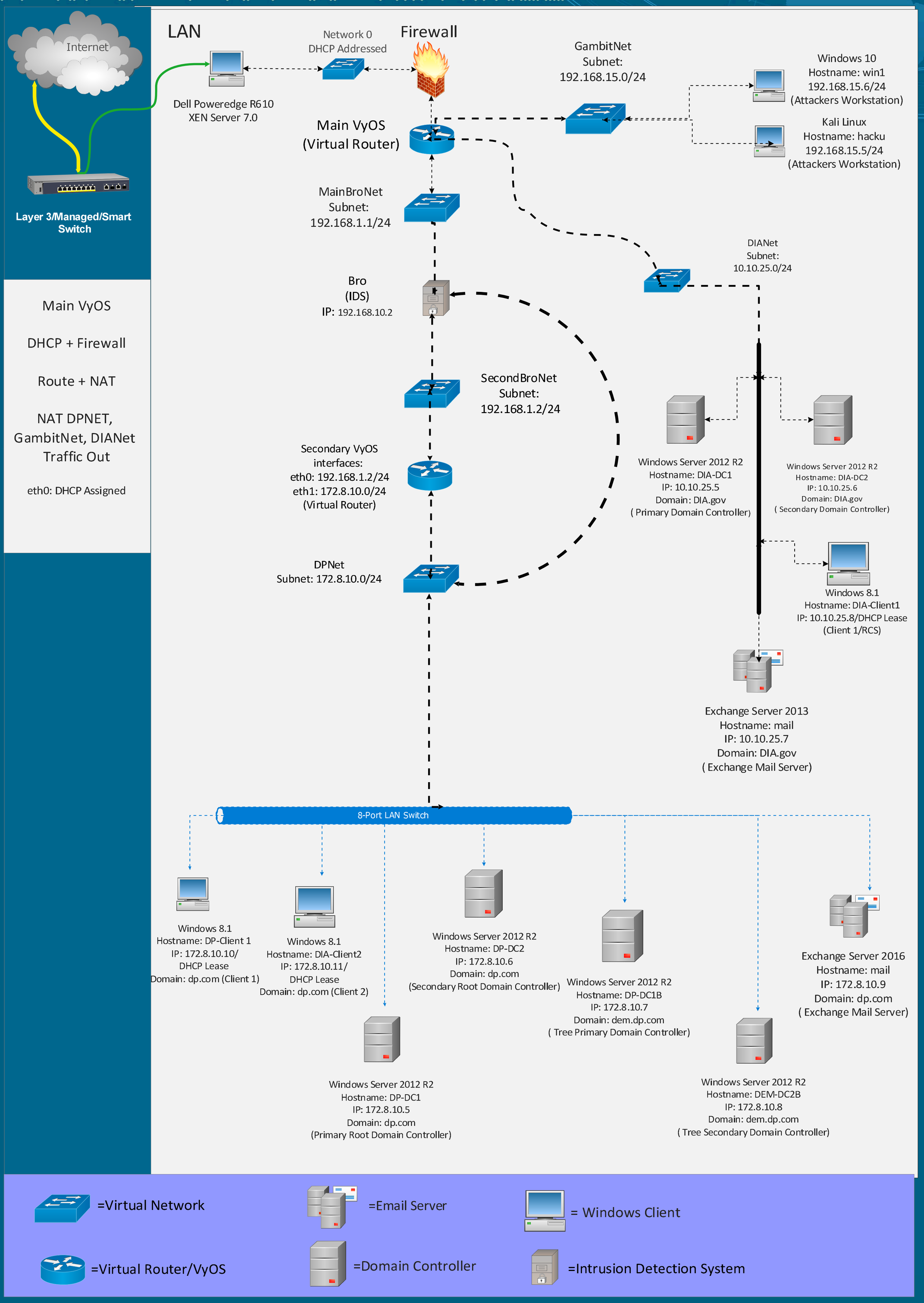
The Center for Cyber Defenders

Expanding computer security knowledge

Tracer Fire 7 System Design

Justin Njenga, Bowie State University; Joshua Russ, Voorhees College; Montrey Freeman, Allen University;

Project Mentor: Kim Tah, 9315



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-XXXXC.