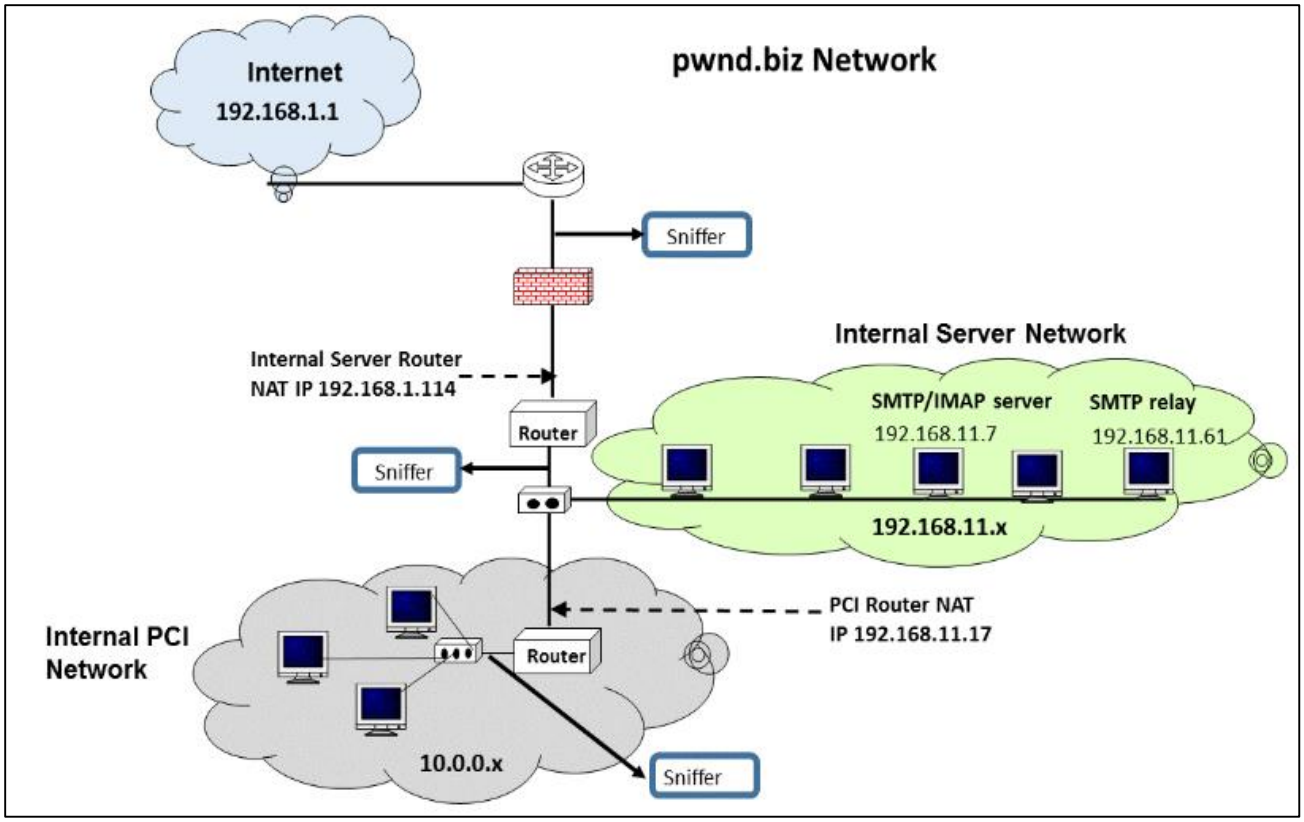
Boston Puzzle 3

Introduction: This puzzle involves a site known as **pwnd.biz**. As the name suggests, it is a security nightmare, run haphazardly without trained IT and security personnel. There has been an incident on the network and your challenge is to investigate what happened and create a comprehensive and coherent incident report.

A network diagram has been supplied. There are three sniffers in the network from which packets have been captured. Keep in mind that Network Address Translation (NAT) is performed on IP addresses when outbound traffic is passing through the internal server network router as well as when outbound traffic is passing through the internal PCI network router. Outbound traffic seen beyond the PCI network and before the internal server router has a single NAT transformation, while outbound traffic seen outside the internal network server router has double NAT transformation when the origin is inside the PCI network.

Helpful Information:

Internal PCI Network IP addresses:	10.0.0.x	internal.pcap
Internal Server IP addresses:	192.168.11.x	inbetween.pcap
Internet Simulation IP addresses:	192.168.1.x	external.pcap



Much gratitude and appreciation for the generous people who created and support the site **www.fakegenerator.com** for the capability to generate various types of records, at no cost, that were used for this exercise.