Track A Challenge Guide

Mission Statement

ACK-ME is a fledgling online social media site whose goal is to bring people together through social posts, pictures, videos and even dating. While ACK-ME does not store any financial data, it does hold a plethora of user data such as email addresses, birthdays, places of residence, employment history, friends, relatives, private photos/videos, and other items of data that could be considered sensitive if it fell into the wrong hands. ACK-ME's pledge is to safeguard and maintain all user data to the highest degree while allowing users to communicate, connect, and share. However, their focus on cybersecurity has been somewhat lax, and their administrative practices poor.

Goal

You are tasked with assisting ACK-ME in response to a series of unrelated cybersecurity events that have recently come to light. These cyber defense tasks include general analysis, incident response, and forensics analysis. All of your actions and analysis will be performed from a defensive posture to events that have already occurred or are currently ongoing.

The goal of your response and analysis of these events is to discern what happened by analyzing forensics data, traffic captures, and logs while also responding to current infections and other system or network maladies.

Scope

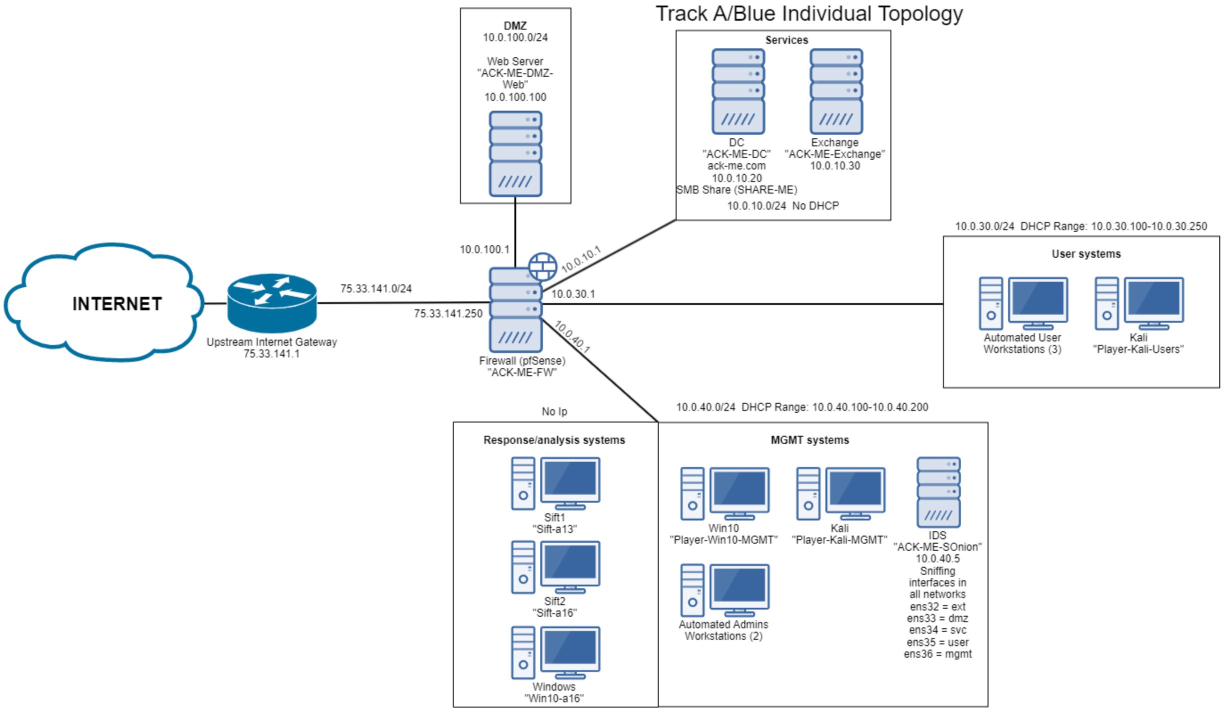
All systems within the ACK-ME network topology are in play. Additional systems containing incident data may be referenced and used for further analysis. The organizational network remains in use during your analysis and investigation. All analysis and investigative methods and included tools are authorized. However, as the network is operational, you should not make any changes to security devices or shut down/restart any systems unless specifically directed to do so.

Topology

This scenario utilizes a common topology. This means several things:

- All challenges will use the same VMs. All VMs are deployed when the first challenge is launched (you may launch any challenge first). New VMs will not be deployed when a new challenge is started.
- Changes to a VM in one challenge will remain when accessing the same VM from another challenge
- You will be able to access all available VMs from any challenge. Some challenges require use of certain VMs. Other challenges are able to be solved using any VM you can access.

Below is an accurate representation of the current network topology, though you will not have console access to every system.



Credentials

VM Name	Username	Password
Domain Controller/Exchange	ACK-ME\Administrator	tartans@1
Player Windows 10	user	tartans
Player Kali (MGMT)	user	tartans
Player Kali (Users)	user	tartans
Security Onion **All tools (sguil, squert, etc)**	user user	tartans tartans
DMZ Web Server	user	tartans
pfSense Firewall **Web console (http://10.0.40.1)**	user user	tartans tartans
SIFT	user	tartans
Analysis Windows	user	tartans