Attack path:

I noticed that /recordings/misc was a valid extension to the website. This also led me to /admin/reports.php which indicated that one of the services that the web server was running was FreePBX 2.8.1.4.

I was able to find exploit 18650 on Exploit-DB which allows for remote code execution. My plan was to spawn a reverse shell using this script, but after several attempts, I realized that the ssl version on the server is incompatible with the ssl version on my machine. As a result, when I run the script, I get the error message "...[SSL: UNSUPPORTED_PROTOCOL..]. I'm not entirely sure how to fix this, so I decide to look for a different attack vector.

Since the web server was running on Elastix, I decided to look into some of those exploits, and discovered that the web server was vulnerable to a data leak detailed by this exploit: https://www.exploit-db.com/exploits/37637. I went to 10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action, looked at the page source and found several passwords. The one that worked was jEhdIekWmdjE, and it allowed me to get root access.