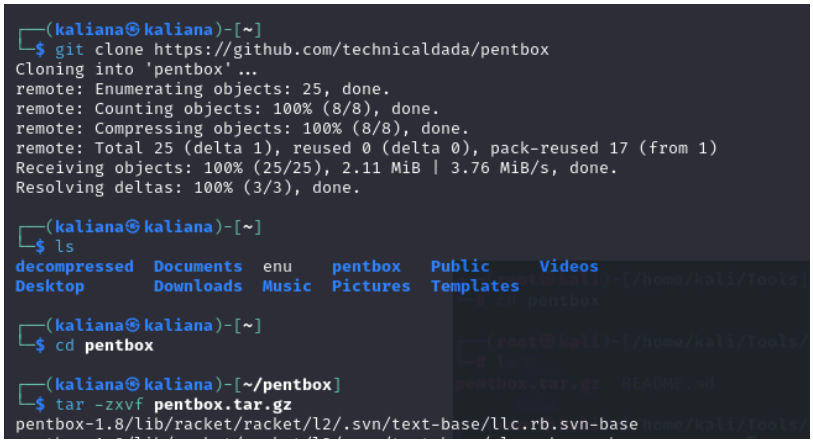
Deploying a HoneyPot with Pentbox

Clay Jones

Objective:

Deploy a honeypot in Kali Linux and use it to detect a Ubuntu machine

Step 1:

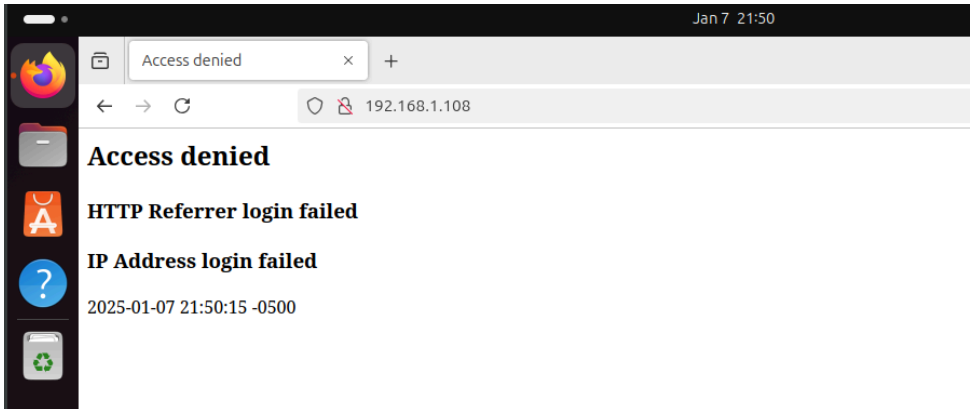


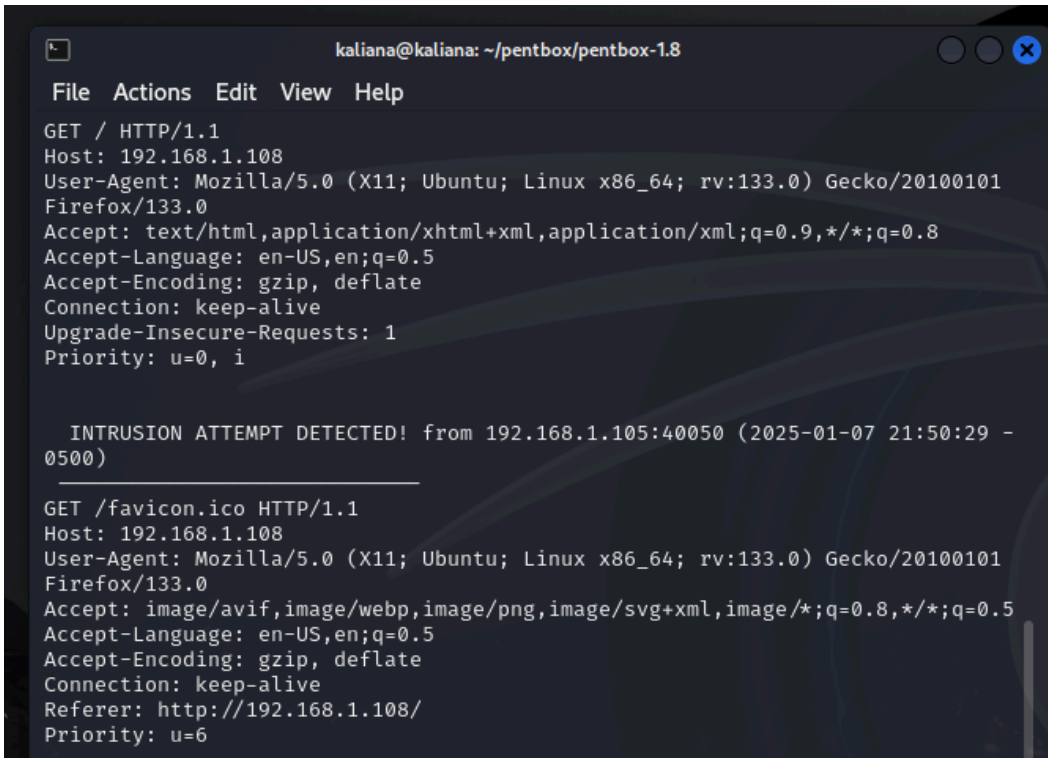
First, I had to clone the pentbox github repository so I could use it. We changed to the new pentbox directory and used tar to extract the archive files. Once that was done , I ran the application.

Step 2:

This is the path used to set up the honeypot. This honeypot simply deploys a HTTP web server. This web server does not contain much but anyone that is snooping around my machine and happens to try and go to my web server, I will be able to capture their information. This includes IP address, operating system, and time.

Step 3:





I visited the web server on my ubuntu (victim machine) using my machine's IP address. I went over to my machine and checked the pentbox and it captured an intrusion attempt. As you can see, it shows different HTTP packet data. With this information, an incident responder can investigate this IP and possibly block this IP from visiting with firewall rules.

Use Cases:

Early Detections, Forensic Evidence, Learn Attack Methods, Distraction for Attacker