Lab-1010 (Challenge): “This is getting heavy, Doc…”

Evidence: lab-1010.pcap

Takeaways: Students will analyze provided network packet capture evidence of a compromised network scenario and attempt to solve “what happened” with as much detail as possible.

The scenario:

Dr. E. Brown was notified by Strickland’s Incident and Event Management (SIEM) system of a possible breach in his network. He quickly dispatched his Incident Handler to obtain a network packet capture over the period of four days and believe they have most of the traffic. Dr. Brown is seeking YOUR help to understand what happened…should he be concerned?

****

Slacker Alert:
Impersonation Alert: The domain “*ebrown-enterprises[.]com*” was detected as a potential impersonation of the domain *e-brown-enterprise[.]com*.

First Detected: 2020-09-20 00:20:30 UTC
Last Detected: 2020-09-20 00:20:30 UTC
****

e-brown-enterprises.com (Dr. Brown’s legitimate domain)
mail.e-brown-enterprises.com (173.230.154.59)
192.168.88.0/24 (IP space inside Dr. Brown’s network)

What happened?

Timeline of Key Events

Should Doc be worried?

IOCs?