Project: LetsDefend, Brute Force Attack

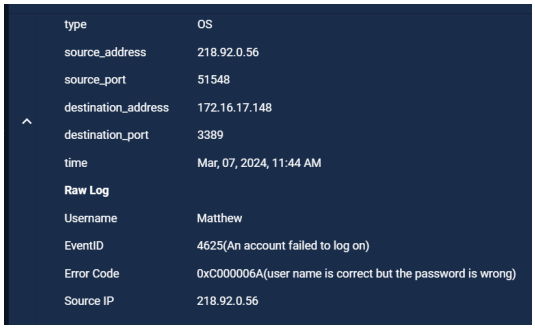
Clay Jones

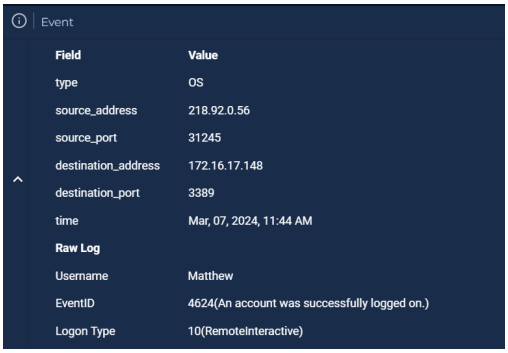
Objective:

A SIEM alert was received describing a brute force attack on an endpoint device. Trace back the artifacts from the log management, treat intel, and the endpoint security manager. Contain the endpoint device if affected.

SIEM Alert:

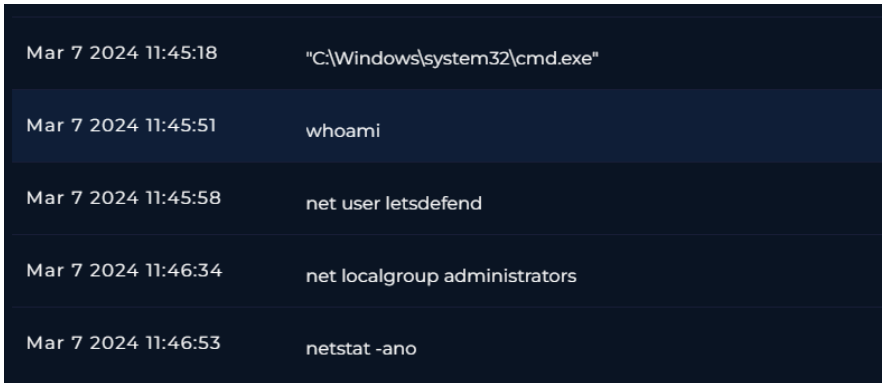
Log Discoveries:

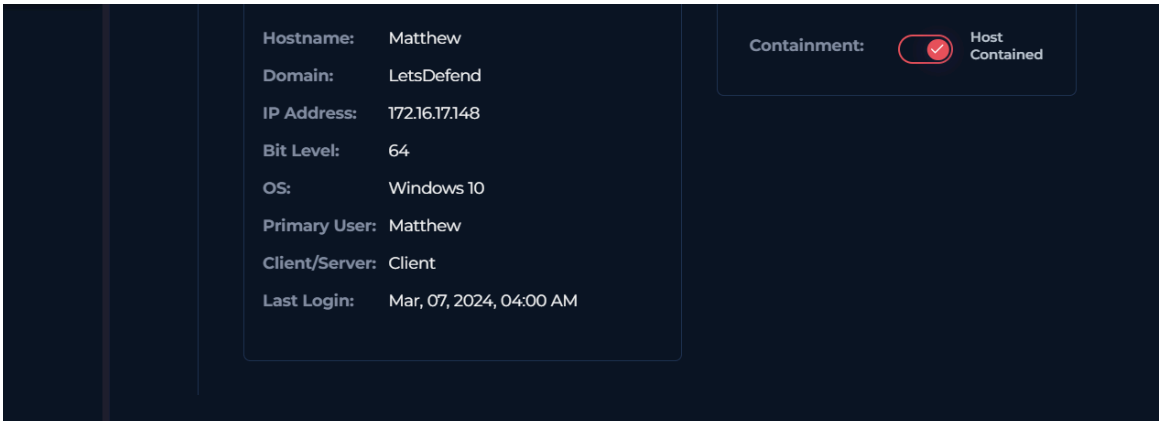


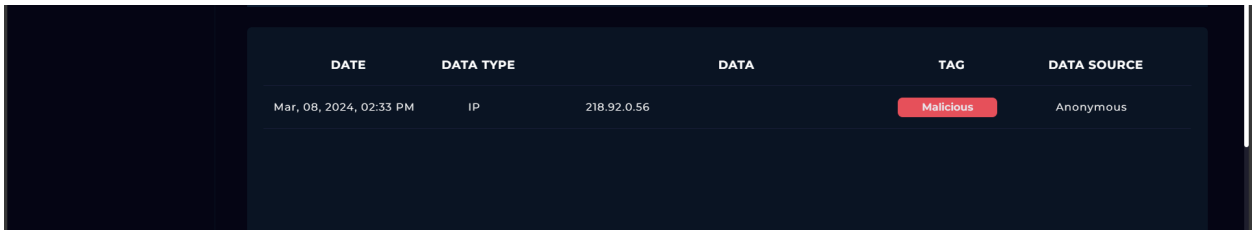


After looking through the log manager, it was shown that multiple attempts were made to brute force into Matthew's account from port 3389. Eventually, the attacker was successfully able to log in after enough attempts.

Host Contained:







Shown from the endpoint security manager, once the attacker gained access, they ran commands such as “whoami”, to confirm they were in, and “net localgroup administrators”, to add, create, or delete a local user group. After seeing such, this host was put in containment and the attacker’s IP was blacklisted and added to the threat intel feed.

Lessons Learned:

To prevent this from happening again, I would strongly suggest:

- Multi Factor Authentication
- Strong password policy
- Account lockout
- CAPTCHA Challenges
- Implement stronger hashing algorithm
- IP Blacklist