

Web Bugs with Deployment Plan

Produced by: Marvin the Martian SOC

Commissioned by: Willey E. Coyote

Date: 11/06/2022

Current Logging Levels on ACME Web Services

After investigation, Marvin the Martian SOC has noted that logging levels on ACME's web services are insufficient. Currently we cannot tell who is accessing the website, web services, internal servers, or who is accessing what. The only breadcrumb trail that we can trace is simply because the IDS and firewall were able to track initial attacks and follow network activity after this.

Solution to Logging Levels

Recommended solutions involve enabling and configuring appropriate logging levels on all web services and internal network services. Installing switches between the general network and network resources would be an ideal way to track who and what is getting in and out of internal servers. Configuring Web servers to appropriately log, and installing web proxies would be a great way to who is accessing our website and web services.