Firewall Findings

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/04/2022

Attacks on ACME systems

Firewalls show beginning 12/12/2017 - 12/29/2017 ACME was subject sustained cyber-attacks and was successfully. Attacks beginning at 4:10pm with Apache injection attacks, on host 10.7.1.20 which were rejected, XSS attacks, and finally a Microsoft server extension buffer overflow which resulted in a workstation belonging to Jessica being compromised. Brute force attempts at 10.7.61.5 were dropped having been recognized as a malicious IP. Successful heart bleed attacks were performed on 12/14 and 12/26 on hosts 13.88.145.74 and 40.78.112.74 respectively. OBJ

Jessica's workstation was then set up as a MITM pivot point, and network enumeration and RCE were executed across the network. Through network and server traversal, the attacker was able to jeopardize Exchange email servers, access Linux file servers, parse PHP information and inject malicious code into the " userjournals_menu" plugin for our SQL servers. Workstation belonging to Thomas was also successfully taken over, and the attacker was able to elevate privileges for both users and successfully navigate all our systems.