Acme Vulnerability Scan

Produced by: Marvin the Martian SOC

Commissioned by: WIley E. Coyote

Date: 11/03/2022

Vulnerability Scan Results

Initial scans do not have much to show. On paper, from vulnerability scanning with both Nessus and Nmap to find running services we do not show very many services running that would be exploitable. Research into security practices by Cyber Stooges is where ACME's greatest vulnerabilities are to be found.

Figure 1 Nessus Scan on network

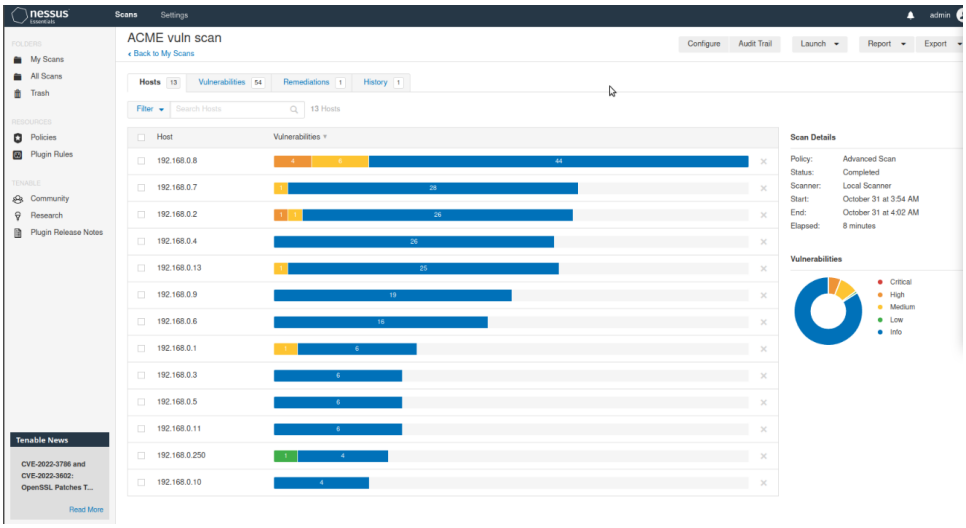
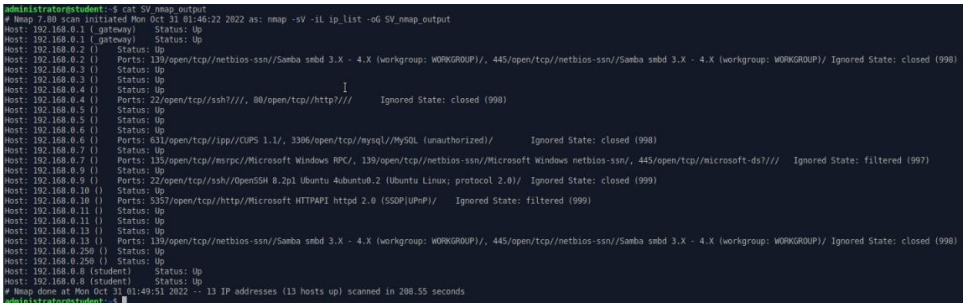


Figure 2 Nmap service scan from inside network.



Other Findings

While scans did not yield much, cursory searching of the website reveals glaring security information in the clear, seemingly used as a security team internal blog post, exposed on open web.

(http://acmecompany.us/) lists all hardware, software, and cloud assets. This is as bad as it gets, inviting intrusion and could be reasonably argued in courts as deliberately exposing confidential information. Along with all assets being listed, critical security flaws in our systems are also listed. Including and not limited to, failure to maintain asset ownership leading to lack of non-repudiation, no PLOP, no access control, IAM being disorganized, and lack of compensating controls.

Figure 3 assets in the clear

Hardware Assets:

Cisco Identity Services Engine
Cisco Firepower
Cisco ASA 5500
Ubiquity Wireless and Network Equipment

Software Assets:

What's Up GOLD
Splunk Enterprise
Active Directory
Windows Print Server
Adobe Connect Server

Cloud Assets
OKTA IdP
Zoho Password Management Suite
Microsoft Teams
One Drive
Office365

Multiple teams, more TBD, including Legal, Compliance, the Systems teams, and PR, must act as fast as possible before any further leaks can continue. All information posted to the site must be removed, validated, remediated and a source must be determined if possible. Hashes are to be taken of company software assets, including internal code, and cross checked across dark web, paste bins, github, and anywhere else that may be of interest. This is to be done ASAP.

Network traffic is to be always monitored to determine a baseline for the next year; deep packet inspection is to be done by the SOC to determine if there are any C2 beacons on the network. DLP technologies are to be installed on determined devices, and network

segmentation to be implemented, to separate confidential information from the rest of the network and disallow access to the internet. A DMZ with a is to be set up with all crucial servers, and investigations will be done on the servers once taken off network to determine of migration to new hardware in the case of rootkits on servers is necessary.