

# Acme Vulnerability Scan

Produced by: Marvin the Martian SOC

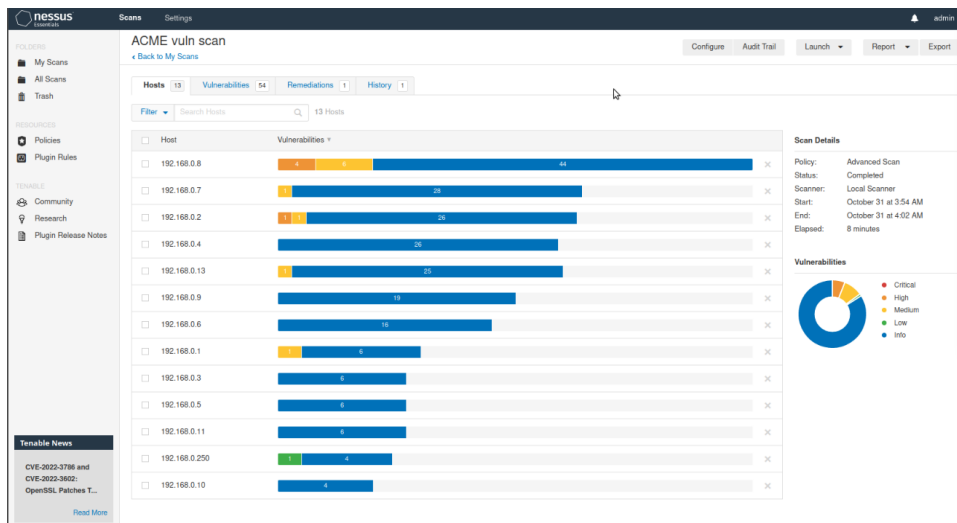
Commissioned by: Willey E. Coyote

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.**

```

administrator@student:~$ cat SV_nmap_output
# nmap 7.80 scan initiated Mon Oct 31 01:46:22 2022 as: nmap -v -iL ip_list -oG SV_nmap_output
Host: 192.168.0.1 (gateway) Status: Up
Host: 192.168.0.1 (gateway) Status: Up
Host: 192.168.0.2 () Status: Up
Host: 192.168.0.2 () Ports: 139/open/tcp/netbios-ssn/Samba smb 3.X - 4.X (workgroup: WORKGROUP), 445/open/tcp/netbios-ssn/Samba smb 3.X - 4.X (workgroup: WORKGROUP)/ Ignored State: closed (998)
Host: 192.168.0.2 () Status: Up
Host: 192.168.0.3 () Status: Up
Host: 192.168.0.4 () Status: Up
Host: 192.168.0.4 () Ports: 22/open/tcp/ssh/ssh, 80/open/tcp/http/http Ignored State: closed (998)
Host: 192.168.0.5 () Status: Up
Host: 192.168.0.5 () Status: Up
Host: 192.168.0.5 () Status: Up
Host: 192.168.0.6 () Status: Up
Host: 192.168.0.6 () Ports: 631/open/tcp/ipp/CUPS 1.1/, 3306/open/tcp/mysql/MySQL (unauthorized)/ Ignored State: closed (998)
Host: 192.168.0.7 () Status: Up
Host: 192.168.0.7 () Ports: 135/open/tcp/msrpc/Microsoft Windows RPC/, 139/open/tcp/netbios-ssn/Microsoft Windows netbios-ssn/, 445/open/tcp/microsoft-ds/ Ignored State: filtered (997)
Host: 192.168.0.9 () Status: Up
Host: 192.168.0.9 () Ports: 22/open/tcp/ssh/OpenSSH 8.2p1 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)/ Ignored State: closed (999)
Host: 192.168.0.10 () Status: Up
Host: 192.168.0.10 () Ports: 5357/open/tcp/http/Microsoft HTTPAPI httpd 2.0 (SSDP|UPnP)/ Ignored State: filtered (999)
Host: 192.168.0.11 () Status: Up
Host: 192.168.0.11 () Status: Up
Host: 192.168.0.13 () Status: Up
Host: 192.168.0.13 () Ports: 139/open/tcp/netbios-ssn/Samba smb 3.X - 4.X (workgroup: WORKGROUP), 445/open/tcp/netbios-ssn/Samba smb 3.X - 4.X (workgroup: WORKGROUP)/ Ignored State: closed (998)
Host: 192.168.0.250 () Status: Up
Host: 192.168.0.250 () Status: Up
Host: 192.168.0.8 (student) Status: Up
Host: 192.168.0.8 (student) Status: Up
# nmap done at Mon Oct 31 01:49:51 2022 -- 13 IP addresses (13 hosts up) scanned in 200.55 seconds
administrator@student:~$

```

## 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.