Assuring Accurate Asset Inventory

Lloyd Powell
March 28, 2018

Table of Contents

1. Introduction

The company wants to determine how many assets are connected to the network.

1.1 Problem Statement

This company doesn't know their assets so they cannot begin the proper cyber security practices. The company needs someone to document the activity on the network. First, the company has to know what devices are connected to their network. From there they can determine what devices are important to them and which assets have vulnerabilities.

1.2 Concepts

There are several key components to share with the company so they have a clear understanding of the network activity. The network scan will provide the company with IP Addresses, the Internet protocols, open ports, versions, and other valuable attributes. These findings will help them understand which machines are vulnerable to attacks.

2. Assets

2.1 Network Scan

These are the statistics from the network scans done on the Backup, Security-Desk, and Workstation-Desk machines. The scans showed six different hosts: Administrator, Kali, Mail, Files, tracker, and backup.

(1) The Backup machine(Linux) is running five TCP servers and four TCP6 (version 6) servers all listening on local address. It is also running six UDP servers and five UPD6 (version 6) on the local address
(2) The Workstation-Desk machine(Windows) is running twenty-three TCP servers all listening on local address. It is also running twelve UDP servers listening on the local address

(3) The Security-Desk(Kali) scan found two hundred fifty-six IP address. There are six different hosts. The chart shows the different hosts and their attributes.

2.2 IP Chart

IP (Class B Private)	Hostname	Asset Type	Description	Service	Open Ports	Protocol
172.16.30.2	Linux Default Gateway	DNS	A secure shell. Used for file transfers and creating the domain names	ssh,domain,http	22,53,80	tcp
172.16.30.5	Windows	Computer			22	tcp
172.16.30.6	kali	Security-Desk	A secure shell	ssh	22	tcp
172.16.30.21	mail.daswebs.com	Mail Server	Used for retrieving emails.	ssh,smtp,http,imap	22,25,80,143	tcp
172.16.30.32	files.daswebs.com	File Server	A computer connected to a network with shared disk access.	ssh, kerberos-sec,netbios-ssn	22,88,139,749	tcp
172.16.30.77	tracker.daswebs.com	Tracker Server	World-Wide-Web server.	http	80	tcp
172.16.30.79	backup.daswebs.com	Backup server	Assists the firewall by attaching Portmapper protcol to connections	ftp,ssh,rpcbind	21,22,111	tcp
172.16.30.101	Workatation-Desk	File Sharing	Microsoft-DS SMB file sharing	msrpc, netbios-ssn, microsoft-ds, nrpe	135, 139, 445, 5666, 49153, 49154, 49155, 49157	tcp

3. Security Concepts

For this assignment I used the command line network scans: Netstat, nmap, and Zenmap. To begin, I had to use the command <ip addr show> to show the machine's IP address. The IP address began with 172, a Private Class B IP Address. I had to analyze the information to find out which protocols in the Internet protocol suite were being used. I could also see which services were listening on the machine. All of the information gathered would help the company find out which devices that they knew and didn't know they had. Then they can determine the value of the asset. They can understand how they need to set controls. In order to prevent attacks sometimes the software needs to be updated, but to know this you need the version number. It is important that companies secure their information and maintain their

confidentiality, integrity, and availability. This process will make the company know themselves so they can prepare for attacks.