Network Asset Manager (NAM)

by

Eric Schmidt, Zach Robinson, Aaron Markvan

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

The author grants to the School of Information Technology permission
to reproduce and distribute copies of this document in whole or in part.

DocuSigned by: Eric Schmidt 62DD3AC393DD4CE...	4/17/2017
Eric Schmidt	Date
DocuSigned by: 763BE2CF2E754FB...	4/17/2017
Zach Robinson	Date
DocuSigned by: C0C66CC0BC7D499...	4/17/2017
Aaron Markvan	Date
DocuSigned by: Brian Verkamp B7D52A3504374A8...	4/17/2017
Brian Verkamp, Faculty Advisor	Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2017

Table of Contents

Table of Tables

Table of Figures

Abstract

The average person has 3-4 devices connected per network. Network Asset Manager (NAM) is an application that allows for devices within a network to be displayed and viewed graphically via a network map. The NAM application assists in the management of the devices on a particular network. The visual network map allows for easy interpretation of network infrastructure and the network scans provide comprehensive system information about devices on the network (operating system (OS), computer name, open ports, etc). Users can store this information in a database and create reports based off the scan results. Less than 40% of organizations conduct full-network active vulnerability scans more than once per quarter.[1] NAM scans determine out-of-date software or potential security vulnerabilities and help harden networks. This application is an affordable way for IT personnel in smaller businesses to actively scan and manage their networks.

Introduction

Network scanning is the process of gathering information about the systems and devices connected to a particular network. This scanning is used for assessing the security of a network and maintenance of the systems. There are many different reasons to scan a network and return information about it. A few examples are: vulnerability, port scanning, host discovery, and network analysis. All of these are important because they will help an administrator determine the health and performance of their network.

Project Description

The average person has 3-4 devices connected per network. Network Asset Manager (NAM) is an application whose goal is to allow for easy management of these devices on a network in smaller businesses and organizations. NAM allows for a network to be viewed graphically on a network map allowing for easy management of network infrastructure. The visual network map provides comprehensive system information about devices on the network (OS, Manufacturer, Model, etc.) which allows the user to see out of date software and potential security vulnerabilities. Less than 40% of organizations conduct full-network active vulnerability scans more than once per quarter.[1] The goal of NAM is to provide an easy and affordable alternative for IT personnel in smaller businesses to conduct vulnerability scans and effectively manage their networks.

Problem

The problem Network Asset Manager faces is vulnerabilities in enterprise networks that may not be found by the user. Less than 40% of organizations conduct a full-network vulnerability scan more than once per quarter. Many breaches that have occurred happened because there was a vulnerability in the network that existed for weeks without anyone noticing. The Network Asset

Manager team is aiming to provide a fast and cost friendly tool that will give organizations helpful information about their network and what measures to take to secure it.

Technical Elements

Network

The network will consist of multiple hosts and servers located at Amazon Web Services (AWS). The networks hosts will be running Windows 10 and Windows Server. The network will be split into different subnets. We will be using Windows Server to help manage users, group policy, and permissions on the network. Only administrators on the network will be allowed to execute the scan.

Sandbox

We will be using AWS and this provides us with virtual machines that can use multiple versions of Linux and Windows operating systems.

Software

NAM will be developed using primarily Java with the Eclipse IDE. Eclipse was chosen as it is the most widely used Java IDE and would provide the most support for what the team is wanting to accomplish. Other languages used will also include C++ and Python, which are both supported by Eclipse. The team will also be using Nmap which is an open source application that also provides an API that is closely related to the goal NAM is trying to accomplish. Other software will include SQL Server Management Studio and Microsoft Windows Server on AWS.

User Profile

There are three potential users for the Network Asset Manager application. See *Figure 1 User Profile* for additional details.

PROJECT: Network Asset Manager
POTENTIAL USERS: ● System Administrators ● IT Office Personnel ● Network Security
SOFTWARE, INTERFACE, AND RELATED EXPERIENCE: Network Asset Manager will primarily target system administrators, small business IT, and network security personnel. These individuals should have experience using common operating systems and software used to scan networks. Our targeted users should have a basic understanding of the potential threats and vulnerabilities found on a network and be able to remove these threats if needed. Users should understand what a network infrastructure looks like and how it functions. The targeted users should have experience with the following protocols, software, and hardware: ● Network Scanning Software ● Windows Operating Systems ● Network Infrastructure Software ● Database Management ● Security Protocols
EXPERIENCE WITH SIMILAR APPLICATIONS: All of our potential users most likely have experience with similar applications such as: anti-virus, database, and device management software. Additionally, these users should have experience with basic command line functions to obtain system information.
TASK EXPERIENCE: IT personnel will have experience with various tasks related to managing a network and keeping it secure. This requires a basic understanding of IT or related knowledge. In the case of small businesses, there may only be one individual that manages every aspect of IT within the business. This usually requires adequate knowledge related to software, networking, network security, and system administration. Due to this, having proper experience with IT systems is required.

System Administrators will have expert experience with much of the IT technology required to manage a network infrastructure. Like IT personnel, this will require an understanding of system admin roles, as well as having an understanding of basic networking and network security related tasks. Database management knowledge will also be required as much of the information about the network will be stored in a database storage system.

IT Security personnel will primarily require experience in dealing with security vulnerabilities and potential threats. A basic understanding of networks and interpreting network infrastructure is also required as this will primarily be the way in recognizing potential threats. Basic database management skills are also needed as much of the security information will be stored in a database system.

FREQUENCY OF USE:

As a system administrator, it is important to know vulnerabilities are present as soon as possible. This tool should be used to scan a network at least once a month. Additional scans should be executed when deemed necessary. If the system administrator has any doubts about the security of their network, a scan is recommended.

KEY PROJECT DESIGN REQUIREMENTS THAT THE PROFILE SUGGESTS:

- User friendly interface
- Display technical system/device information
- Visual network map
- Centralized device management
- Archive network scans into database
- Generate reports

Figure 1: User Profile

Use Case Diagram

The below figure is the Use Case Diagram for NAM. It shows two potential types of users and the different ways those users will interact with the application.

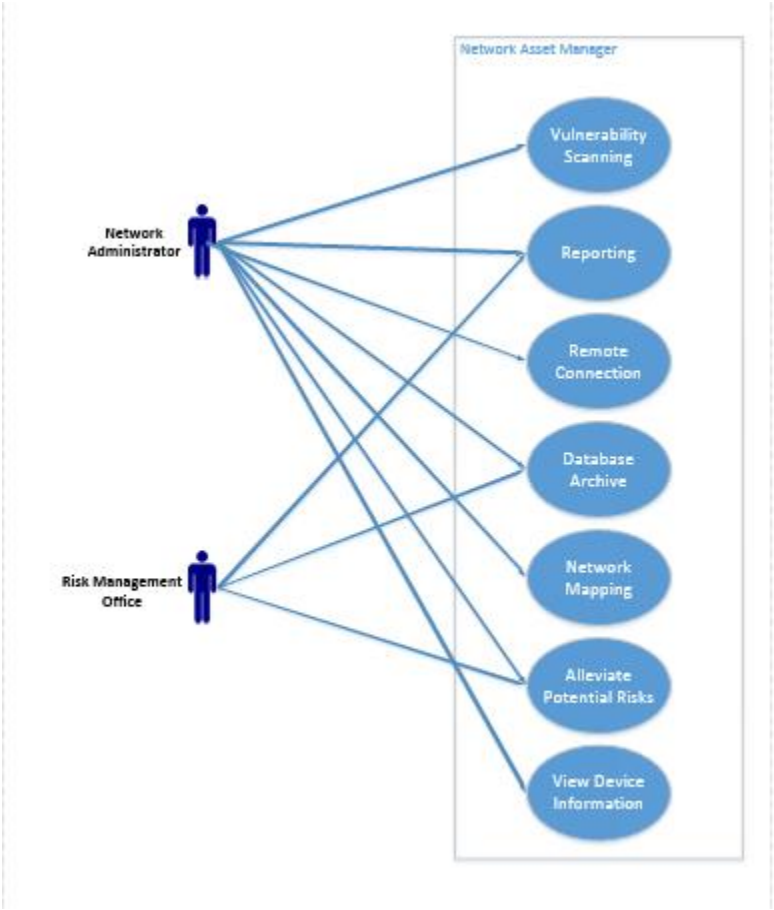
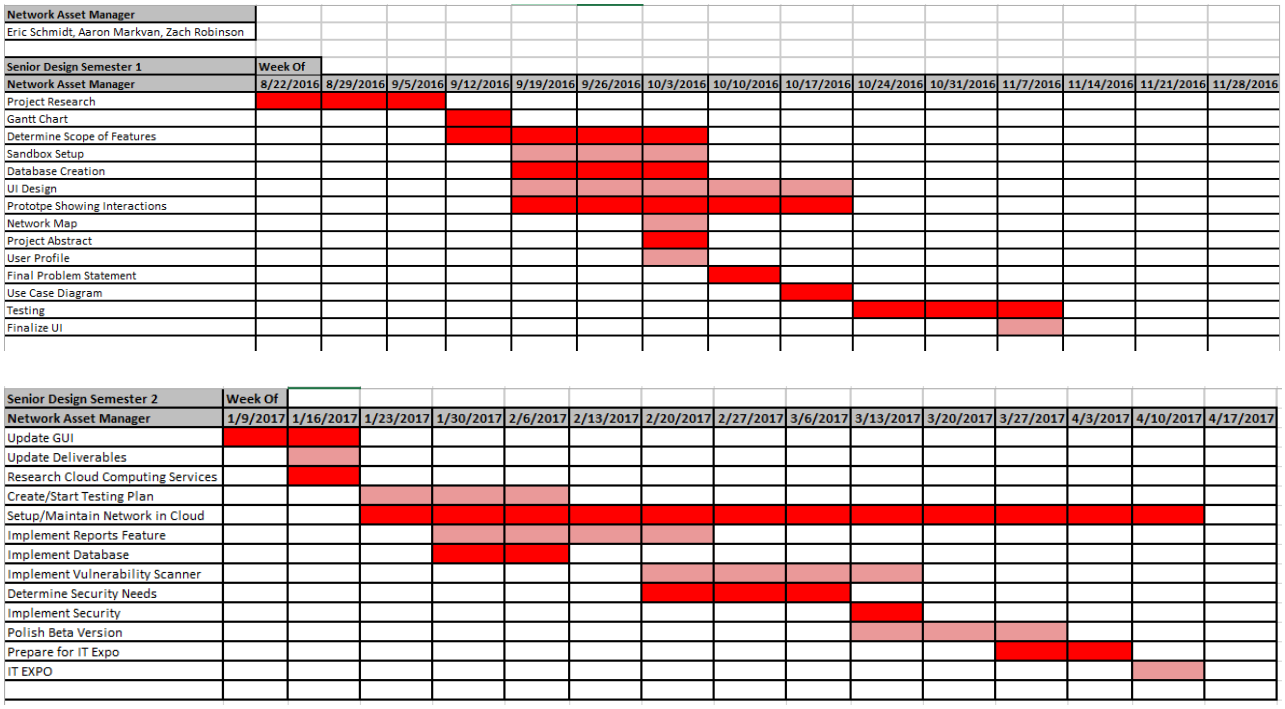


Figure 2: Use Case Diagram

Gantt Chart

The figure below is our Gantt chart for both the first and second semester.



Network Asset Manager																
Eric Schmidt, Aaron Markvan, Zach Robinson																
Senior Design Semester 1	**Week Of**															
Network Asset Manager	**8/22/2016**	**8/29/2016**	**9/5/2016**	**9/12/2016**	**9/19/2016**	**9/26/2016**	**10/3/2016**	**10/10/2016**	**10/17/2016**	**10/24/2016**	**10/31/2016**	**11/7/2016**	**11/14/2016**	**11/21/2016**	**11/28/2016**
Project Research															
Gantt Chart															
Determine Scope of Features															
Sandbox Setup															
Database Creation															
UI Design															
Prototpe Showing Interactions															
Network Map															
Project Abstract															
User Profile															
Final Problem Statement															
Use Case Diagram															
Testing															
Finalize UI															

Senior Design Semester 2	Week Of														
Network Asset Manager	**1/9/2017**	**1/16/2017**	**1/23/2017**	**1/30/2017**	**2/6/2017**	**2/13/2017**	**2/20/2017**	**2/27/2017**	**3/6/2017**	**3/13/2017**	**3/20/2017**	**3/27/2017**	**4/3/2017**	**4/10/2017**	**4/17/2017**
Update GUI															
Update Deliverables															
Research Cloud Computing Services															
Create/Start Testing Plan															
Setup/Maintain Network in Cloud															
Implement Reports Feature															
Implement Database															
Implement Vulnerability Scanner															
Determine Security Needs															
Implement Security															
Polish Beta Version															
Prepare for IT Expo															
IT EXPO															

Figure 3: Gantt Chart

Deliverables

Table 1: Project Deliverables Due Dates. The table below lists out the different deliverables our group decided to include for the project.

Sandbox Setup	**10/7/2016**
Database Creation	**10/7/2016**
Network Map	**10/21/2016**
Prototype UI Design	**10/21/2016**
Prototype Showing Interactions	**10/21/2016**
Testing	**11/7/2016**
Finalize UI	**11/11/2016**
Update GUI	**1/16/2017**
Research Cloud Computing Services	**1/16/2017**

Testing Plan	**2/6/2017**
Create Network in Cloud	**2/6/2017**
Database Implementation	**2/6/2017**
Reports Feature	**2/20/2017**
Vulnerability Scanner	**3/13/2017**
Application Security	**3/13/2017**
Beta Version	**3/27/2017**

Table 1: Project Deliverable Due Dates

Budget

Table 2: Project Budget. The table below presents an estimated project budget using real-world costs. Due to this being our senior project, the actual cost of developing this application will be $0 as much of the services used are free or are provided by the University of Cincinnati. NAM is expected to be open source and free after development.

No.	Item	Unit, Each	Unit Price	Item Total
	Networking			
1	Labor	320	$35.00	$11,200.00
	Software			
2	Labor	160	$35.00	$5,600.00
	Microsoft Windows Server	1	$1,172.64	$1,172.64
	Supplies			
3	Misc. Supplies	-	-	$
	Estimated Total			$17,972.64
	Actual Total			$0.00

Table 2: Project Budget

Testing

Overview

This section will go over the testing that was conducted by the NAM development team and what procedures were included.

Scope

The scope of this testing plan is to endure that the NAM application works correctly when the administrator conducts the scan of an IP address.

Objective

The objective of this testing plan is to verify that tasks included in the NAM application are working correctly. The tests are intended to ensure that one important task is functional, so that the next task can also be tested.

Results

The below table (Table 3) shows the results of each one of the tests that were conducted by the NAM development team.

Application Testing Checklist			
Application Name	Network Asset Manager		
Procedure	Expected Result	Pass/Fail (P/F)	Actual Results/Comments
Application Functionality			
Execute simple scan of the network	Yes	P	Able to retrieve computer IP addresses and other basic information

Execute heavy scan of the network	Yes	P	Able to retrieve more in depth information such as open ports, OS info, etc.
Execute scan from text file	Yes	P	Able to execute scan by importing an IP Table
Dynamic network map functions	Yes	P	Map is able to be manipulated by the user and shows IPs
Information saved to database	Yes	P	Scan information is properly saved to the database
Display device information	Yes	P	Scanned devices are shown with all of their device information
Save scan report	Yes	P	Reports successfully saved to host
Open scan report	Yes	P	Open report successfully
AWS Services	Yes	P	AWS platform tested for communication between hosts. Hosts are able to ping each other.

Table 3: Application Testing Checklist

Network Diagram

The figure below is our network diagram for NAM. It shows how the applications interacts with hosts and how the data is returned to the user who initiated the scan.

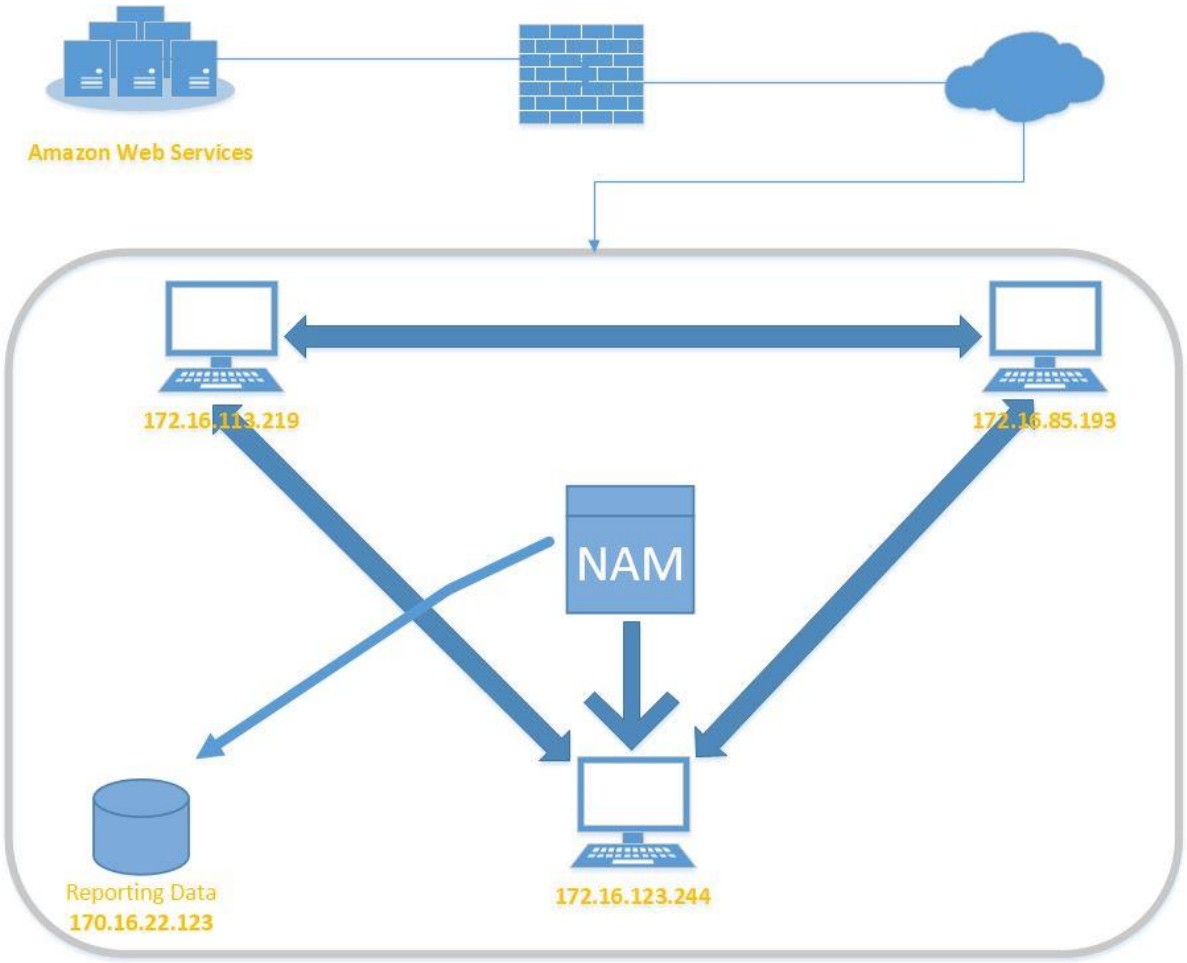


Figure 4: Network Diagram

Conclusion

When we first started defining the scope for our project, we thought of many different features to include in the application. As we did more research the scope narrowed due to our timeline and the complexity of the features. Security features and the vulnerability scanner are the most important features that we included. The scanner was the hardest thing to implement and took the longest amount of time. As a group we wanted to create something that none us had ever done before and I believe we succeeded with Network Asset Manager (NAM).

References

1 *2015 Cyberthreat Defense Report: North America & Europe.* CyberEdge Group, LLC. 2015.