Vulnerability Analysis Report

For

Prepared by:

Security Gurus
123 Mockingbird Lane
Austin, TX

Joe Flintrock, MCSE
Gerry Sandstone, CEH, CCIE

Scan Manifest

Customer:	ACME
Scan Identifier:	External Scan Internal Scan
Date:	Internal scan: April 8, 2012 External scan: April 15, 2012
Time Started:	Internal scan: 7:30 pm External scan: 11:30 pm
Tools	Retina 5.17.2901 Nessus 1.1.9 Nmap 6.25
Scope	Internal scan: xxx.xxx.xxx/xx External scan: xx.xx.xx/xx
Description:	The purpose of this vulnerability scan is to collect supporting evidence for the Security Assessment. This scan is not intended to scan all known hosts and identify all vulnerabilities. The results of this scan will be used to ascertain the types of security counter measures and controls are in place and their effectiveness.

Table of Contents

Executive Summary

Scope:

The internal and external vulnerability scans are used as a tool to gather data to assess the effectiveness of current security control measures taken at the system level of ACME's network. Further, this data will be used as evidence to support findings and recommendations found in the Security Assessment document. The purpose of the scan is not to determine all vulnerabilities, therefore a representative sample of servers were scanned. The internal scan took place at the headquarters location. Our scanner was plugged into a switch that resides inside ACME's network. The purpose is to bypass external security controls and counter measures to get a detailed look at system configurations. The xxx.xxx.xxx/xx network was chosen by ACME's IT staff for the internal scan. The external scan's purpose is to see the security posture through the eyes of the Internet user. The point is to know what a hacker would see if he were trying to probe ACME's network. The IP address chosen by ACME's IT staff was xx.xx.xx/xx.

Approach:
When performing vulnerability scans, there is always a risk of affecting a system causing it to degrade in performance or causing it to stop functioning all together. We mitigate this risk by conducting interviews with the client to understand the design of the network and its systems. On production systems, critical servers are identified and decisions are made whether or not to include them as targets for the scan. This decision depends on the risk tolerance of the customer and potential impact to the customer in the event the scan causes the system to degrade in performance or stop functioning. Other measures taken prior to the scan include: coordinating with the client to provide personal to be available during the scan, notifying internal and external groups that may be affected by the scan.

The vulnerability scan has three phases: network discovery, vulnerability assessment, and manual checks (optional). The first two phases require the use of scanning tools. The tools used to scan ACME were nmap, Retina, and Nessus. Since a representative sample from ACME's network was scanned, the Network Discovery phase only involved discovering live hosts on the targeted networks. The tool nmap is used to determine hosts on the network. The output from phase one is inputted into phase two. Retina and Nessus are then used to scan theses hosts for vulnerabilities. Phase three was only conducted on the external scan.

Findings from the internal scan and external scan will be used to generate the following report. Nmap, Retina and Nessus generate their own reports and will be made available.

Findings:

The results from the internal scan and the external scan are listed below.

- **Internal Scan**
  - **Ineffective Procedures**: The results from the internal scan indicate that the current security configuration procedures are ineffective.
  - **Old Passwords**: There are several accounts with passwords older than thirty days and some are even close to a year old.

- **Old Patch Levels**: Many systems reported the need for patches and updates that have been published for at least thirty days.
- **Unnecessary Services**: Many systems had multiple ports open indicating the presence of unnecessary server services.

- **External Scan**
  - **FTP Anonymous Access**: Manual checks indicated that a review of perimeter security is needed. The ftp server on **ftp.ACME.com** allows anonymous access. This site has a multitude of files that appear to be at least confidential in classification. One file contains user accounts of which some belong to terminated employees.
  - **Open Email Relay**: The email server (mail.ACME.com) allows open email relaying. Anyone in the world has the ability to use this server to create and send emails.

Recommendations:

The following recommendations are based only on the results of the vulnerability scans. Vulnerability scanning is one tool to assess the security posture of a network. The results should not be interpreted as definitive measurement of the current security posture. Other elements used to assess the current security posture would include a code review of applications, password cracking, denial of service attacks and tools that automate common attacks. The tools we used contain modules that can be included or excluded. Some features were not turned on due the level of risk tolerance. Some of the modules not included were: Denial of Service scans, automated common attacks, and password cracking.

Account maintenance, Patch management and system configuration are the main security elements that need to be addressed. ACME needs to address each of these issues at their security policy first. Processes, whether they are manual or automated, can then be researched, tested and implemented. After the processes are defined, methods, and tools to measure compliance and auditing should be implemented. All three of these issues can be resolved with a good policy, procedure, proper administrative tools, and adequate staff. The degree of automation can be addressed by risk tolerance, budget, and limitations of the automated solution sets.

Before long-term solution sets can be recommended, a thorough audit of user accounts, system requirements needs to be conducted. There are immediate solutions that can be quickly implemented. There are various resources for server hardening: SANS Security Focus, Titan, Bastille, etc… A baseline configuration for each build should be determined from which adjustments can be done a server-by-server basis. Security patches are freely available from the major vendors such as Sun, Microsoft, and Red Hat. Download the relevant patches, test and install them. There are no quick solutions to gain control of user accounts. The solution starts with a good policy that is enforced and monitored.

Internal Vulnerability Assessment

Scope

The internal vulnerability scan was conducted on the xxx.xxx.xxx/xx network. This network was deemed by ACME personnel to contain a representative sample of the various host configurations that exist throughout ACME's network. The tools used to conduct the vulnerability scans were: nmap, Nessus, and Retina. A reconnaissance scan of the target network revealed xx hosts. All xx hosts were scanned.

Summary of Findings

Detailed findings of the external scan can be found and studied in the raw reports generated by the scanning tools.

The findings from the internal scan do not take into account perimeter security controls or counter measures. The scans are conducted behind such controls and counter measures with the purpose of determining a clearer picture of the target host's security posture. The severity levels attached to the findings assume that perimeter security has been breached or has malfunctioned. Security in depth is a common practice that mitigates the risk of a security breach by not depending on one layer of defense. A penetration test would be the next step to determine which of the internal findings could be exploited from the Internet.

The findings clearly show that the current procedures to define and maintain user accounts and system configuration are ineffective. There are multiple accounts with passwords that are at least 45 days old, do not expire, or accounts that have never been used. Multiple hosts were found to not have up to date security patches. Some of which would allow worms like code red to exploit the vulnerable host. Extraneous ports and services were also a wide spread occurrence.

Summary Table

Finding Title	HIGH	MEDIUM	LOW	Comments
Account Security	0	4	2	Results are from two hosts. 13 accounts found
System Security	79	84	87	These findings combine configuration and patch issues
Total	79	88	89	

Recommendations

There are three areas that need to be addressed as a result of the internal scan: system hardening, patch management, and user account management. Each one of

these areas should be first addressed at the Corporate Security Policy. Before procedures can be defined to address the corporate security policies, high-level solutions will be defined that address each of the three findings. Solution sets will then be listed and mapped to each finding area.

Solutions:

Ideally ACME needs a solution that has the ability to work across multiple operating systems and starts from the security policy down. This tool(s) would allow the system administrator to create a policy, and push it across the network. The tool should monitor for changes in security configurations, alert administrators when new patches are available, and make it easy to create, delete and manage accounts. The reality is that only a few tools exist with multiple management features. Furthermore, automation cannot make decisions of how to test and integrate new policies and security patches. There is no one tool that replaces the need for a good process and a good system administrator to carry out his/her job. Therefore, our solution sets will address tools that have multiple functions and tools with only dedicated functions.

The majority of the findings were either patch or configuration related. It is clear from the scan results that the current methods to harden ACME's servers are ineffective. System hardening is a process that addresses the following issues:

- Minimizes ports and services
- Restricts permissions to mandatory accounts
- Enables logging of host and application events
- Enables countermeasures at the network layer
- Enforces password policies
- Manages remote access

ACME has an immediate and a long-range need to harden their systems. The scan results clearly show that unnecessary services are running on multiple systems. An immediate fix would be the use of freely available scripts such as Titan and Bastille. Other resources include SANS and Security focus guidelines for hardening. ACME could create baseline-hardening configurations and push them out to their Unix and Linux systems. Windows 7 has the ability to create and push security profiles through out multiple domains. System hardening is an ongoing process and difficult to manage in large muliti-platform networks. ACME should consider using a tool that enforces the security policies from a central management station.

Several hosts reported the absence of critical security patches. These patches are freely available from the vendor of the operating system or the application. A policy should be created to define who is in charge of making sure patches are up to date and who is responsible for installing the patches. The policy should also state how ACME would remain abreast of new patches. A corresponding process should then be created to define the types of systems and the locations of where security patches can be obtained. An immediate solution would be to setup a directory in the intranet as repository for patches. An administrator would then be charged with the task to keep the files current, filter out irrelevant patches, test the relevant patches and then deploy them. The administrator should be on all relevant mailing lists. Another option would be to evaluate a tool that sends customized alerts of new patches, versions and hot fixes.

The results from the scans and external probing clearly show that user accounts procedures are ineffective. Multiple accounts have passwords older than 45 days and some older than a year. Some accounts have never been used and the ftp.ACME.com site lists a user account that maps to a terminated employee. Account management starts with the security policy. It should be instituted as a corporate policy and any System Admin toolset could be used to manage it if used properly. This goes back to mixing least privilege access with an audit trail for all account creation and deletion. An effort to gain control of accounts would be to start with a full and exhaustive audit of all current accounts. Technologies such as Radius, LDAP, single sign on, etc. could then be evaluated on how to maintain control and manage user accounts.

Solution Sets

This table is not an exhaustive source of vendors and solution sets. Its purpose is to demonstrate the variety of tools on the market and the solutions they offer.

Key:
SH = System Hardening
PM = Patch Management
AM = Account Management

SOLUTION SETS	SH	PM	AM	COST	TIME Install/Manage	COMMENTS
SANS	X			M	H	Various guidelines on system hardening
Securityfocus	X			L	H	Various guidelines on system hardening
Titan	X			L	M	Solaris hardening script
Bastille	X			L	M	Linux hardening script
NetIQ	X		X	H	M/L	Enterprise security solution
PatchLink.com		X		?	M	Cross-platform patch discovery. Enterprise-wide
UpdateExpert		X		?	M	Microsoft only
UserManagemeNT			X	M/H	M/L	Windows only
SailPoint			X	H	M/L	Identity management
Site Minder			X	M/H	M/L	Multiple platform support Single sign on Authentication
LDAP/Radius			X	M/L	M/L	Multiple vendors Single authentication solution
Red Hat Network		X		L	H/M	Red Hat systems only
Microsoft Updates		X		L	H/M	Windows systems only
Sun Solv		X		L	H/M	Solaris patches only

External Vulnerability Assessment

Scope

The external vulnerability scan was conducted on the xx.xx.xx.xx/24 network. This network was deemed by ACME personnel to contain a representative sample of the various host configurations that an outside user could view from the Internet. The tools used to scan this network were: Nmap, Nessus, and Retina.

Summary of Findings

The findings from the external scan produced very few results. It appears that process to implement and administer perimeter security is effective. However, three exceptions were discovered. An FTP server with anonymous access contains information about user accounts and customer data that should not be readable to the world. When an email server allows relaying, emails can be spoofed from anyone using this vulnerable server. This also allows some one to abuse the system resources. Names and contact numbers were found through zone transfers from the DNS servers. This information would be one step in an attempt to social engineer user account information from third parties or the help desk.

Recommendations

The solutions to the three problems are inexpensive and would involve little time to implement. The ftp server ftp.erot.com should not allow anonymous access with the type of information currently on it. Have the system administrator turn off anonymous access. Email relaying was found on mail.ACME.com. Look up the vendor documentation on the email server to find the commands to turn off relaying. This is a task that the system administrator will be able to accomplish. The DNS administrator needs to edit the contact information to reflect a help desk or emergency contact and remove any employee's name and phone number

Appendix A: Security Gurus Scanning Methodology

This service scans a Security Gurus Customer site via the Internet from outside its perimeter security controls to search for vulnerabilities that may exist within specifically identified components accessible from the Internet, including firewalls, web servers, and exposed hosts.

The vulnerability scanning was performed using common off-the-shelf (COTS) tools and proprietary tools developed by Security Gurus. The COTS tool in use is Nessus v6.25 for Linux.

Security Gurus probes public sources of information to point out to our customers what type of information they are making easily available. Unethical attackers can access this information as easily as Security Gurus Security Services can.

The information test cases access public services in an attempt to gather reconnaissance information about the target hosts.

Port Scan/OS Detection

A port scan is the process of using an automated tool to attempt to locate all TCP or UDP ports on a host that are advertising a service. This information is useful to a hacker because it lets him or her know what services are running on a host. When they know what services are running, they know what services can be attacked.

The port-scanning program performs OS detection. The program queries a host using a collection of packets, and determines from the results of those packets what vendor and version of OS is running on the host.

Vulnerability Scan

Tools are used to scan for and detect vulnerabilities that exist within a customer's site. If the tools can detect the holes, the customer can implement the necessary patches, updates, or workarounds to plug the holes. This provides one less avenue for an attacker to use when attempting to compromise a customer system.

The scanning test cases are searching for information about services offered by the machine or potential application vulnerabilities.

Security Gurus also offers exposure to DOS ("Denial of Service") test cases. DOS test cases attempt to take the machines out of service by sending malformed or floods of packets.

Appendix B: Defense in Depth Philosophy

Defense in Depth is a concept that relies on total security throughout a web commerce site. Defense in Depth means that from the perimeter to the back-end connections of a network, security is considered and applied at a rigorous level.

Some of the activities that are performed for a defense in depth security approach are perimeter rule set analysis and optimization (either for a front-end packet filtering router or firewall), server (OS and application) hardening, inclusion of network and host based IDS solutions, vulnerability scanning, penetration testing and comprehensive audit log review.

Perimeter rule set analysis and optimization ensures that only the traffic that is specified in the site's security policy is allowed to pass. Server OS and application hardening removes interfaces from the existing machines to minimize available avenues of attack. Network and host based IDS solutions alert the site's operational personnel when a breach is attempted or successful. Vulnerability scanning and penetration testing serve to demonstrate that the site has no holes that could be exploited by an attacker. Comprehensive audit log review ensures that a security incident has not occurred in the past, and gone unnoticed.

The vulnerability scan detailed in this report is a moment in time analysis. When changes are made to an operational site, new vulnerabilities may be introduced. It is in the sites best interest to be scanned and tested regularly for vulnerabilities.