GSNA Practical v4.0

Option 1
Topic 1

Auditing with NMap, LC5, and Oracle Password Guesser

Lora Danielle
12/18/04

Abstract

In today's computing environment, security is of the utmost importance. Many organizations have been running for long periods of time without seriously addressing security concerns. In order to address this problem, government standards like the Federal Information Security Management Act (FISMA) have been created to help organizations secure their environments in an organized and standardized manner.

The goal of this document is to provide the security community with usable examples of system audits. The information below originates from an enterprise environment that is implementing security measures as an enterprise-wide effort. To better understand the system that they are preparing to secure, LFO has requested that an internal network audit be performed utilizing the NIST SP 800-26 checklist. The audit begins with and identification of the system and a formal scope of work.

The following document illustrates three of the audit points that were discovered and addressed in an actual audit. Each audit point identifies a potential risk for an unsecured system, and then follows a repeatable step-by-step procedure to reveal the current state of the system being audited. The final point for each audit item details the results from the actual audit.

The document comes to an end with a summary of each audit point and the effect the audit had on the organization.

Introduction

Auditing a device or a system is an essential part of maintaining a secure environment. Whether auditing a single computer or an enterprise network, the first step of determining the scope of the audit is crucial. The scope allows for clearly discernable limits, and keeps the audit results comprehensible and straightforward. Once the scope has been decided on, a risk analysis will put a value on the device or system that is being audited. If the system is at high risk, but has a low value, then it would not make sense to invest in the most expensive security system available. On the other hand, if something is at high risk, and is very valuable, then a certain amount of investment for security purposes should be expected. Once the scope and the risks have been defined, the audit can be performed. Taking a methodical approach to discover vulnerabilities on a device or system can prove to be invaluable. Documenting and analyzing the results will provide the organization with precious data that can be used to secure their systems and make their enterprise a safer place.

The following includes three examples taken from an exhaustive enterprise audit. The first audit deals with the strength of network passwords. The second audit discusses the account vulnerabilities of a default installation of Oracle. Finally, the third audit examines the identification of rogue network services.

Identifying and Testing a System for Audit

1.1. Identify the system to be audited

This information is from an audit I performed of the internal network for a Large Federal Organization (LFO). The organization is using the NIST 800-26 IT Security Self-Assessment to create a baseline for their network security standards, which will help them to meet their goal of being in compliance with FISMA standards. Using the NIST 800-26 guidelines, LFO requested an audit of their current internal security practices and for recommended security practices that would allow LFO to meet or exceed the current FISMA standards.

The network being audited is headquartered in the Washington DC (WDC) regional area. There are two other large sites in the Northeast, and there are smaller sites throughout the country and in some International areas, as well.

The scope of this audit includes only the servers and workstations on the internal network. The internal network sits behind a complex system of firewalls, and the enterprise also has a DMZ network for all public-interfacing servers. The firewalls and computers in the DMZ are administered in the WDC site by a separate Engineering group and are out of scope for this audit.

The main network infrastructure is comprised of Windows NT servers. The network is being upgraded to Windows 2000, both on servers and workstations. The servers provide network services including DNS, DDHCP, and WINS. Application servers include Microsoft Exchange 5.5 servers, and Oracle and SQL database servers. The majority of workstations have been migrated to Windows 2000 Professional.

The internal network is critical to the daily functioning of LFO. E-mail and Blackberry are used constantly by users who need to communicate with each other and share data. File servers hold the data for thousands of individuals who use the information for their daily work. Oracle and SQL databases hold critical data for the work that is done at LFO. All of these systems are considered to be mission critical. It is imperative that the internal network can support this traffic, and that the servers have a minimum amount of downtime; otherwise the entire organization fails to run properly.

The systems that will be referred to in this document include the network passwords that users use to log on to the internal network, namely their workstations; the Oracle application on servers that reside on the internal network, in regard to the default Oracle account and password information; and the network traffic that is on the internal network and the services that correspond to that traffic.

Network passwords are one of the most elementary, yet most valuable, aspects to network security. As thousands of users log on to their workstations every day, they are putting in credentials that allow them access to the most basic resources of their company: the data. Although typing in an account and password can become almost second-nature to most users, in terms of security a successful logon can be equated to crossing a castle's moat by using the retractable bridge. It is essential to use complex passwords on a network because if an unauthorized user somehow gains access to a valid network user account and password, then an unauthorized user has just walked into the enemy's castle straight through the gate! The role of the password is to protect the network from unauthorized use, but weak passwords only create a false sense of security. Because the password protects the network, it should be as complex as the data is valuable.

LFO utilizes Oracle databases to store and manipulate the personnel data for hundreds of thousands of people in the United States, and around the world. The information stored in the Oracle databases is the most sensitive and valuable information in the organization. There are currently 47 Oracle servers in production at LFO, and these servers contain financial data for the hundreds of thousands of individuals that LFO serves.

For a number of years, the network at LFO has grown without much guidance and with very little documentation. When a server or service was needed, it was put on the network without any fanfare. Servers were installed without Installation Guidelines, resulting in hundreds of servers configured differently, based on whatever best practices the technician felt like implementing, or whatever time constraints were being placed on the server. Some servers would use Windows Update to automatically install service packs and hot fixes, while some would not. Almost every server was installed with IIS, even though there was no reason for it to be installed on the internal network. LFO currently has a staff dedicated to engineering enterprise-wide solutions for the network, in contrast to the previous staff of server administrators and technicians, who had a much smaller view of the system. This staff of engineers will be responsible for monitoring services as they come up on the network, and verifying that they are appropriate and necessary. This audit will provide the engineers the documentation they need to begin the process of eliminating unnecessary networks services and documenting the current state of the network.

1.2. Current State

LFO is currently working in an “unknown” state of practice. The system and network administrators spend too much time troubleshooting server problems and have no useful documented history of the system. Because no password policies are in place, users often share their weak and well-known passwords to give co-workers access to information that should be restricted. There is no way for administrators to tell what is happening on the network, and there are too many application administrators that install and run services on servers that the network administrators are unable to keep up with the changes. Because the administrators spend so much time running around fixing seemingly individual types of problems, there is little time for documentation and overall network improvement.

The goal of the security audit is to provide the administrators with an overall view of their network and the security risks that are dominant within the system.

Risk Analysis for Item #1 – Complex Password Policy

1.1. Threats and their Capacity to Inflict Damage

- **System** – Internal Network
- **Vulnerabilities** –
    - Weak passwords allow for easy social engineering, and easy cracking
    - Server administrators share admin accounts and passwords
    - Users share accounts and passwords
    - A complex password policy exists, but is not enforced
- **Likelihood of Exploitation** – High
- **Value of the Asset** – High
- **Potential Impact** – High

- **Confidentiality** – Unauthorized users that gain administrative or escalated privileges by guessing or cracking passwords have unlimited access to the sensitive data stored on the network
- **Integrity** - There is no accountability for unauthorized changes made to the network or servers; Sensitive data can be copied, changed or deleted without authorization

1.2 Vulnerability and Impact for Risk

Item Number 1:
Network password policies are not enforced

Risk:
NIST SP 800-26 defines the risk associated with accounts and passwords as a Technical Measure by stating “Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users.”

Testing Procedure / Compliance Procedure:
Use password auditing utility to verify passwords match the enterprise security policy (e.g., passwords utilize alpha numeric, upper/lower case, and special characters).

1.3 Impact of vulnerability

Often referred to as the “keys to the kingdom,” passwords are used to secure data on networks. When a user logs into the network, he or she is granted certain permissions on the network to access certain resources.

In this case, LFO has determined that their data is “sensitive but unclassified (SBU).” As a result, they would like to utilize a user-id and password method of accessing the network and they also want to be sure that the passwords meet a level of complexity that will provide a reasonable amount of protection against being cracked. LFO has a security policy that dictates how passwords should be constructed to meet security requirements, but it is believed that few users follow the policy in actual practice. By auditing the organization’s passwords against their policy, compliance with the policy can be determined and represented in a quantitative manner to management.

To begin the password audit, it is important to know what the organization’s policy contains. From there, passwords can be audited against the organization’s specific standards. In this example, LFO has the following password policy requirements in place:

> Use of passwords is required in LFO. Passwords provide access to LFO systems and resources for authorized users while denying access to unauthorized users.

Your User-id and password identify you, and they must be protected to ensure no one can impersonate you. Don't share your User-id or your password with anyone. Do not write your password down; instead, create a password that you can remember.

- You must change your system password every 60 days. As a service to you, the system will notify you when it's time to change your password. If you do not change your password, you'll be locked out of the network until you contact the help desk to receive a new password.
- If your account is inactive for more than 35 days on any of our systems, your access will be revoked, and you will have to reestablish your account.
- You can't reuse your password for six iterations.
- Your password may not contain your user-id or any part of your full name.
- Your password must be at least eight characters long and contain both characters and numbers. For stronger security, choose longer passwords with characters from all four classes.
- A complex password that cannot be broken is useless if you cannot remember it. For security to function, you must choose a password you can remember and yet is complex. For example, Msi5!YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).
- Your password must contain characters from at least 3 of the following 4 classes:

Classes	Examples
1. Upper Case Letters	A, B, C, … Z
2. Lower Case Letters	a, b, c, … z
3. Arabic Numerals	0, 1, 2, … 9
4. Non-alphanumeric ("special characters")	For example, punctuation symbols: ({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=)

Chart 1.1 – Password Character Classes

You can try logging into an LFO system up to three times with different passwords; but, your account will be locked if you don't get in by the third try.

> If this happens, you must call the Help Desk. The Help Desk will authenticate your identity. Once your identity is confirmed, the Help Desk will reactivate your account with a temporary password that must be changed the first time you use it to log in(LFO 1).

1.4. Primary vulnerabilities that could lead to the impact

Management has discovered that users at LFO often share their passwords with each other. This can be a big problem for a number of reasons. If one user is given local administrative rights to a workstation, for example, that user can then go around installing software or disabling anti-virus on all their friend's workstations. Network administrators sometimes log in to servers using another administrator's credentials. This can cause problems with troubleshooting and accountability. If administrative passwords become commonly known, then administrators that may not have rights to particular resources may log on to the network as another administrator and make inappropriate or unauthorized changes to network services and cause problems throughout the entire network. Even worse, if a disgruntled network administrator leaves the organization, but still knows another administrator's password, imagine the havoc that could result if the disgruntled employee decided to create trouble, even if the disgruntled administrator's account is disabled.

Users and Administrators are sharing passwords because there is no emphasis on the importance of having a complex, password that they do not share. In conjunction with enforcing a strong password policy, it will be important that LFO educate the user community in order to delineate exactly why it is important for each user to keep their complex password to themselves.

1.5. Scenario of exposure and means of exploitation for the vulnerability

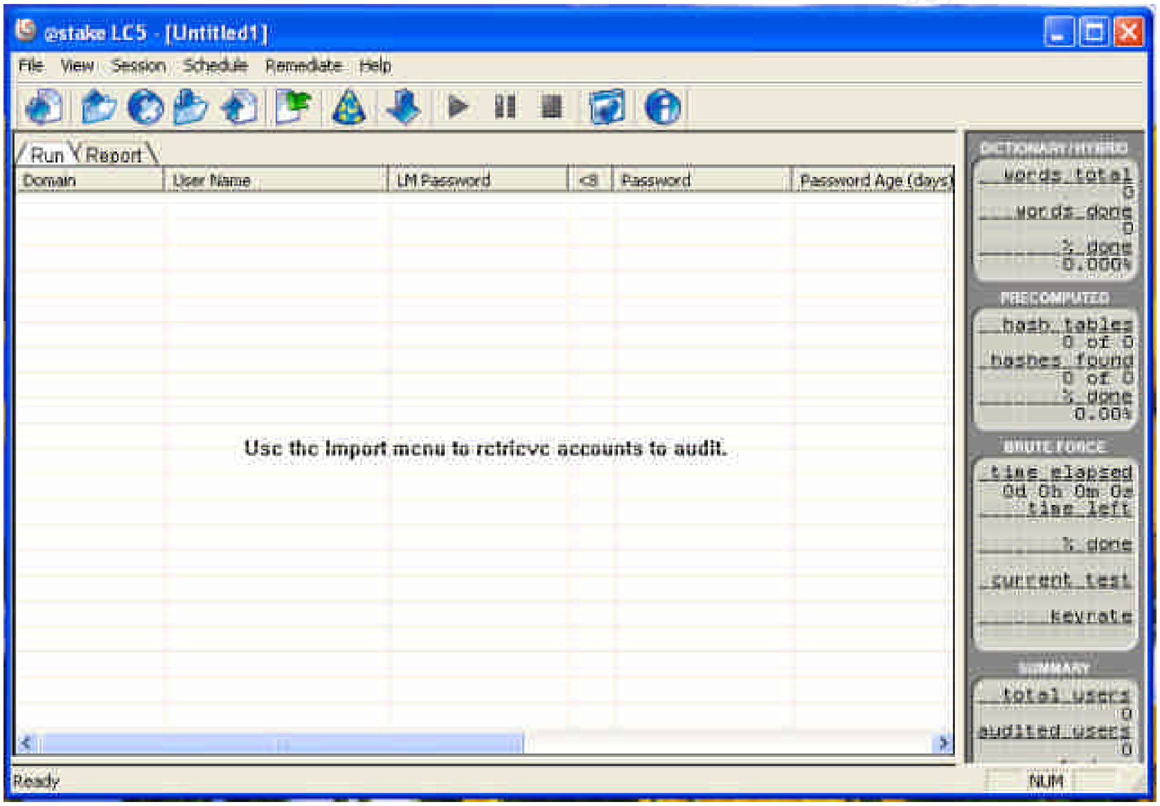
Of course, internal users and disgruntled administrators are not the only concern. If weak passwords are used throughout the network, then cracking or social engineering passwords becomes very simple for anyone interested in gaining unauthorized access to network resources. Consider the embarrassment a corporation would suffer if an unauthorized user was able to gain access to sensitive or proprietary data just by guessing an administrative password! That data could then be posted on the Internet to damage the corporation's reputation, could be used by the unauthorized user for his or her personal gain (like credit card information), or could even be used to attempt blackmail against the unwitting corporation. By educating users and by implementing a complex password policy, an organization has gone a long way to preventing social engineering of passwords, and has made it much more difficult to crack passwords with a cracking utility.

For these reasons, complex password policies are essential for the protection of the data on a network. The above password policy example demonstrates a minimum level of complexity that is appropriate for most networks today.

Testing for Item #1

The first step in auditing a network's passwords involved attaining the organization's password policy document. This document will contain all the information that an auditor will need to determine what criteria should be used for the audit. Once the auditor has the organization's password policy, its use can be verified with a password cracker, like @stake's L0phtcrack.

LC5 is the most current version available from @stake:



Use the Import menu to retrieve accounts to audit.

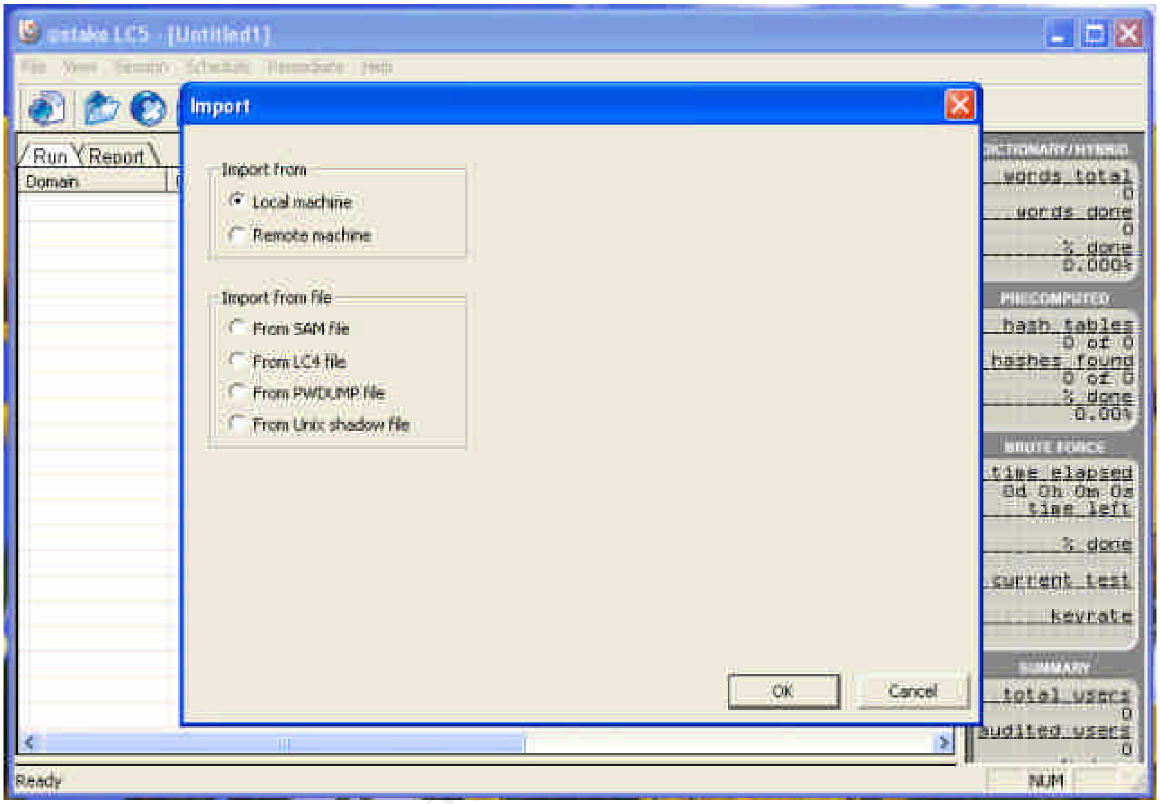
words total 0
words done 0
% done 0.000%
hash tables 0 of 0
hashes found 0 of 0
% done 0.00%
time elapsed 0d 0h 0m 0s
time left
% done
current test
keyrate
total users 0
audited users 0

Step 1: Determine Password Policy Requirements

Determining what criteria to use to audit passwords is usually the most significant aspect in the process. It is never a good idea to try and crack all the organization's passwords, regardless of strength. The point of the audit is to determine if any passwords fall outside the security policy regulations, which is why it is important to be familiar with the organization's specific policy guidelines. In this situation, the audit will look for passwords that are fewer than 8 characters, that contains part of the user-id, or that does not contain 3 out of 4 of the "classes" as shown in *Chart 1.1 – Password Character Classes*.

Step 2: Import Password File from Domain Controller

If you have administrator access to the network, then you can import the password list from the SAM or Active Directory with the LC utility. If you do not, you will need to investigate some of the other options that LC5 makes available for gathering passwords from the network. Here is an example of the screen you will get when you are ready to import a password file into the LC5 application for auditing:



Import

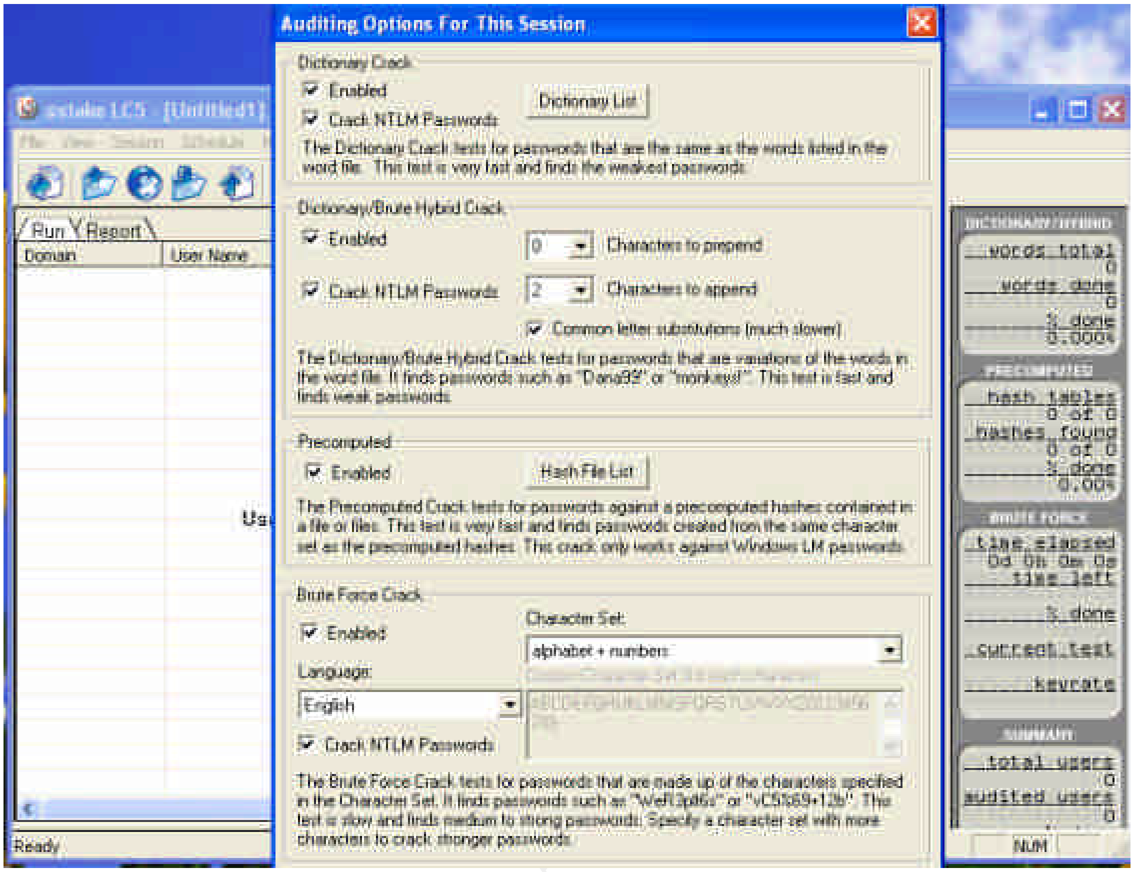
Import from
● Local machine
○ Remote machine

Import from file
○ From SAM file
○ From LC4 file
○ From PWDUMP file
○ From Unix shadow file

In this case the auditor is going to import the SAM file from the Domain Controller. Where the **Import from** option appears, the auditor will choose **Remote machine**, and will choose **From SAM file** under the **Import from** file option. In a later screen, the auditor will enter the IP address of the domain controller that the auditor wants to connect to in order to download the SAM file.

Step 3: Configure Auditing Options Based on Password Policy

To determine what passwords fall outside of the security policy regulations, configure the appropriate options in the LC5 Options tab, shown below:



Auditing Options For This Session

Dictionary Crack

☑ Enabled

☑ Crack NTLM Passwords

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack

☑ Enabled

☑ Crack NTLM Passwords

0 Characters to prepend

2 Characters to append

☑ Common letter substitutions (much slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

Precomputed

☑ Enabled

The Precomputed Crack tests for passwords against a precomputed hashes contained in a file or files. This test is very fast and finds passwords created from the same character set as the precomputed hashes. This crack only works against Windows LM passwords.

Brute Force Crack

☑ Enabled

Language: English

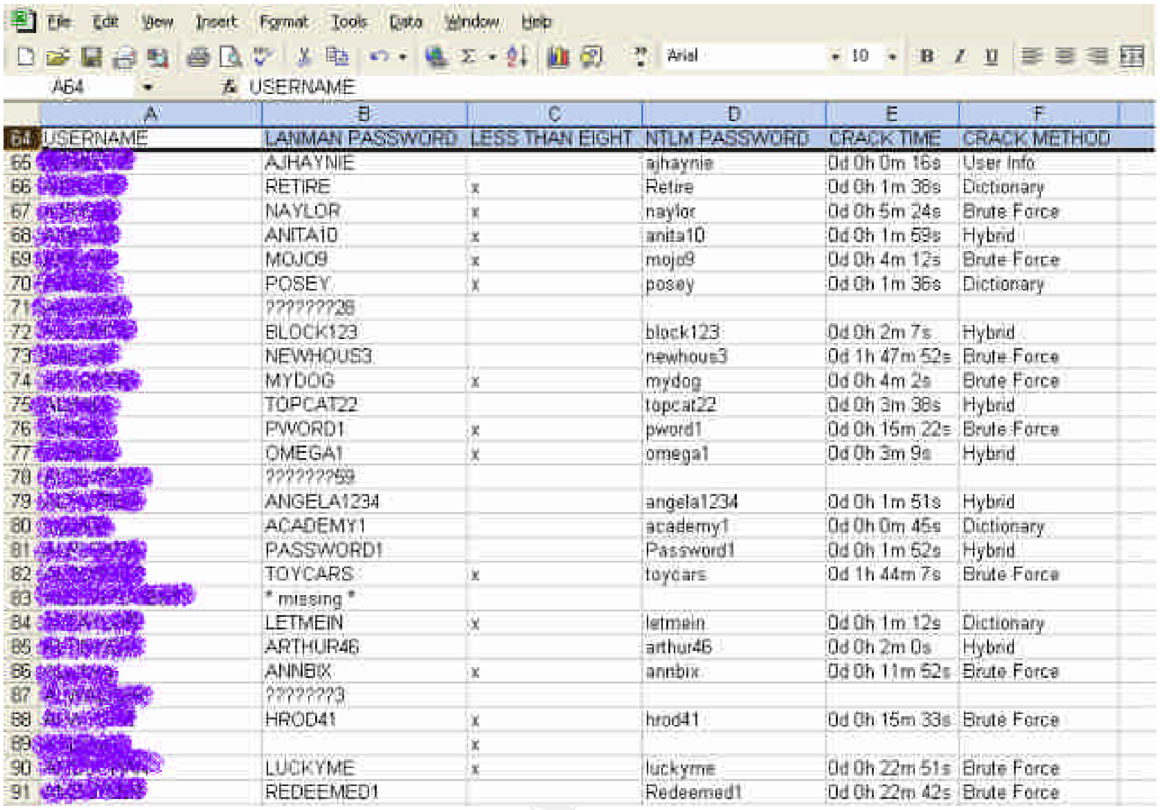
☑ Crack NTLM Passwords

Character Set: alphabet + numbers

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3pt6s" or "vC5%89+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

Depending on the organization's password policy, LC5 can be configured to audit different levels of passwords. In this case, the auditor would select both options under **Dictionary Crack**, would enable the **Dictionary/Brute Hybrid Crack**, would enable the **Precomputed** Hash File List, and would enable the **Brute Force Crack**, as well. The same password file can be saved before it is cracked the first time, then used to run different auditing configurations. For this audit, different scans will be run with different options for the number of characters to "prepend" and "append," and with different character sets for the Brute Force Crack. The auditor will want to collect the different results, and compare the results of the various configurations. When preparing an executive summary of the findings, it is often enlightening to management to see how quickly simple passwords can be cracked, especially if it is one of their own!

Step 4: Analyze the Results



	A	B	C	D	E	F
64	USERNAME	LANMAN PASSWORD	LESS THAN EIGHT	NTLM PASSWORD	CRACK TIME	CRACK METHOD
65	[redacted]	AJHAYNIE		ajhaynie	0d 0h 0m 16s	User Info
66	[redacted]	RETIRE	x	Retire	0d 0h 1m 38s	Dictionary
67	[redacted]	NAYLOR	x	naylor	0d 0h 5m 24s	Brute Force
68	[redacted]	ANITA10	x	anita10	0d 0h 1m 59s	Hybrid
69	[redacted]	MOJO9	x	mojo9	0d 0h 4m 12s	Brute Force
70	[redacted]	POSEY	x	posey	0d 0h 1m 36s	Dictionary
71	[redacted]	???????26				
72	[redacted]	BLOCK123		block123	0d 0h 2m 7s	Hybrid
73	[redacted]	NEWHOUS3		newhous3	0d 1h 47m 52s	Brute Force
74	[redacted]	MYDOG	x	mydog	0d 0h 4m 2s	Brute Force
75	[redacted]	TOPCAT22		topcat22	0d 0h 3m 38s	Hybrid
76	[redacted]	PWORD1	x	pword1	0d 0h 15m 22s	Brute Force
77	[redacted]	OMEGA1	x	omega1	0d 0h 3m 9s	Hybrid
78	[redacted]	???????59				
79	[redacted]	ANGELA1234		angela1234	0d 0h 1m 51s	Hybrid
80	[redacted]	ACADEMY1		academy1	0d 0h 0m 45s	Dictionary
81	[redacted]	PASSWORD1		Password1	0d 0h 1m 52s	Hybrid
82	[redacted]	TOYCARS	x	toycars	0d 1h 44m 7s	Brute Force
83	[redacted]	* missing *				
84	[redacted]	LETMEIN	x	letmein	0d 0h 1m 12s	Dictionary
85	[redacted]	ARTHUR46		arthur46	0d 0h 2m 0s	Hybrid
86	[redacted]	ANNBIX	x	annbix	0d 0h 11m 52s	Brute Force
87	[redacted]	???????3				
88	[redacted]	HROD41	x	hrod41	0d 0h 15m 33s	Brute Force
89	[redacted]		x			
90	[redacted]	LUCKYME	x	luckyme	0d 0h 22m 51s	Brute Force
91	[redacted]	REDEEMED1		Redeemed1	0d 0h 22m 42s	Brute Force

Step 5: Pass or Fail

To tell if a password fails the complexity requirements from the Security Policy, it will be necessary to review the cracked passwords to see if any meet the policy, but were still cracked. For example, the password "Password1" was cracked, but still meets the requirement set in the policy because it has an Uppercase, a lower case, and a numeral. Regardless of the fact that it meets the requirements, it is obviously a weak password and was cracked in less than two minutes. This type of information can be presented to management to stress the importance of utilizing complex passwords that are created in a more secure manner than "Password1." For example, the password "Pass1word" would be more secure, because the number or special character is in the middle of the password, rather than at the beginning or the end. Because it is possible for a password to meet the password policy, but still be cracked in a small amount of time, a Pass/Fail requirement must be taken with a grain of salt. Objectively, as long as all of the passwords meet or exceed the security policy, then the passwords passed the audit. On the other hand, if all of the passwords meet or exceed the password policy, but a large number of the passwords were still cracked in a small amount of time, then it may be a sign that the password policy is not complex enough. The results of the audit will provide management with the ability to make an informed decision regarding the complexity requirements for their organization.

Audit Results for Item #1

After running LC5 against the domain password file at LFO, it was determined that out of 6527 accounts, only 412 were unable to be cracked before the audit was stopped. The remaining 6115 passwords were cracked in less than 2 hours, 9 minutes, and 15 seconds. Although some passwords met the security policy requirements for complexity and were still cracked, the majority of the passwords did not meet the requirements of the password policy for LFO.

Risk Analysis for Item #2 – Default Oracle Accounts and Passwords

2.1. Threats and their Capacity to Inflict Damage

- **System** – Oracle Servers
- **Vulnerabilities** –
  - blank passwords and default accounts are installed by default with the Oracle application
  - Developers are given shared admin accounts to Oracle servers and applications
  - default Oracle accounts and passwords are not changed or disabled
- **Likelihood of Exploitation** – High
- **Value of the asset** – High
- **Potential Impact** – High
  - **Integrity** – Systems can be harmed by users with admin rights who may not be familiar with the operating system; Oracle developers rarely need local server admin rights, and if they do, their account should be person specific, rather than shared, to allow for more user responsibility and accountability
  - **Availability** – Developers with admin rights to the server can make inappropriate changes to the OS that result in system downtime; default user/password combinations can be exploited by malware to change or harm databases resulting in downtime for the application

2.2 Vulnerability and Impact for Risk

Item Number 2:

- Password policies are not enforced on network applications, specifically Oracle.
- Users are given inappropriate levels of access which may result in damage to the data, either by accident or on purpose.

Risk:

NIST SP 800-26 defines the risk associated with accounts and passwords as a Technical security measure by stating: "Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users."

Testing Procedure / Compliance Criteria:

- Utilize an application (Oracle) password auditing utility to be sure that all passwords meet Password Policy requirements.
- Verify that default accounts are changed or disabled. If the accounts are necessary, verify that complex passwords are in use.

2.3 Impact of vulnerability

Like many other applications, the Oracle application comes with default settings that need to be secured before the application becomes available to general users. According to NIST.net, Oracle can install up to 207 default accounts and passwords, although usually a smaller number will typically be installed with most databases. Because these accounts are often overlooked by Oracle and network administrators when the application is installed, one common ways to gain unauthorized access to an Oracle database involves attempting a connection using one of these known default account and password combinations.

As a result, one significant step in ensuring the security of an Oracle database is to be sure that any default account and password combinations are disabled if they are unnecessary. If the accounts will be used, then it is important that the passwords are changed to meet the complexity requirements of the organization's Password Policy.

In this case, securing the Oracle servers was a substantial concern to LFO because the personnel records of hundreds of thousands of people are contained on the Oracle servers. This information is the most sensitive data that the organization is responsible for, so if it were to be compromised, it would cause great embarrassment to the organization, and might even lead to lawsuits if the public was aware of any compromise. The organization had previous incidents of records being manipulated, resulting in financial loss, and is eager to find ways to prevent future incidents.

2.4. Primary vulnerabilities that could lead to the impact

All servers, including Oracle servers at LFO are built and configured by a group of engineers that have a broad general knowledge of networking, but are primarily experienced with the Windows NT/2000 Operating System, and not necessarily the applications they are installing. Because of this, the server is built and the applications are installed with standard default configurations. The server is then passed on to the Oracle group, which is made up primarily of developers, very few of whom have database administration knowledge. This situation causes the servers to be placed into production loaded with sensitive data without receiving any security configurations. Because the developers believed they were administering the servers appropriately, management feels comfortable with the current staff, and sees no benefit in hiring a dedicated database administrator.

2.5. Scenario of exposure and means of exploitation for the vulnerability

With up to 207 default accounts and passwords that can be installed with the default Oracle application, the opportunity for unauthorized access is overwhelming. Users that should have limited access to the Oracle database are often granted administrative rights by the developers, who typically administer the servers and who do not want or know how to decide what lower level of access might be more appropriate. More importantly, any network user that has enough knowledge about Oracle to know about the default accounts and passwords could gain access to the database and leave no distinctive trace. Users in the past have been able to gain access to sensitive data by using inappropriate administrative rights. Regardless of the fact that the administrative rights were granted to them by the administrator of the server, these users do not need administrative rights, and the network administrators are often contacted to perform restores of data that have been deleted or improperly manipulated by these users. It is known that the systems have been compromised in the past, and that it was compromised by internal users with administrative access to the Oracle application.

Testing for Item #2

Deciding which users should have administrative access to the Oracle application is a decision that needs to be sponsored by management and enforced by whoever is performing the duties of the Oracle administrator. Allowing access is a subjective process that is dynamic, and access controls should be reviewed regularly to determine if the rights being given remain appropriate.

Discovering if default accounts and passwords are in place is a different matter, however. Auditing Oracle for default accounts and passwords is very straight-forward and the solution can be implemented immediately upon discovery.

Step 1: Use NMap to Find Oracle Servers

In this particular organization, the network administrators were not in possession of up-to-date documentation that itemized all the Oracle servers currently in use on the network. The first step to auditing the security of the server involves locating each server on the network. An NMap or NMapWin network discovery process can be used to find Oracle services running on the network. Although there are a number of different ports that can be used to identify an Oracle server, in this case the auditor is starting with a scan for port TCP 1525.

One example for finding Oracle services includes using the following NMapWin scan: -sS –PT –p 1521 –O –T 2 –oN “OracleScan.txt” 10.1.1.1-254.

Step 2: Analyze Results of Scan

The NMap scan results should resemble the output below.

Oracle.zzz.lfo.gov on IP address 10.1.1.203 shows that port 1521 is running a service, most likely Oracle.

```
Interesting ports on Oracle.zzz.lfo.gov (10.1.1.203):
Port       State       Service
1521/tcp   open        oracle
The 1 scanned port on rrrlfo (10.1.1.204) is: closed
Interesting ports on  (10.1.1.205):
Port       State       Service
1521/tcp   filtered    oracle
The 1 scanned port on lfoxxx.zzz.lfo.gov (10.1.1.206) is: closed
The 1 scanned port on eeelfo.lfo.gov (10.1.1.207) is: closed
The 1 scanned port on wwwlfo.lfo.gov (10.1.1.208) is: closed
Interesting ports on lfoqqq.lfo.gov (10.1.1.209):
Port       State       Service
1521/tcp   filtered    oracle
Interesting ports on  (10.1.1.210):
Port       State       Service
1521/tcp   filtered    oracle
Interesting ports on  (10.1.1.211):
Port       State       Service
1521/tcp   filtered    oracle
The 1 scanned port on lfoxxx.lfo.gov (10.1.1.212) is: closed
Interesting ports on  (10.1.1.213):
Port       State       Service
1521/tcp   filtered    oracle
The 1 scanned port on xxxxxxx (10.1.1.214) is: closed
Interesting ports on xxxxxxx (10.1.1.215):
Port       State       Service
1521/tcp   filtered    oracle
Nmap run completed -- 256 IP addresses (256 hosts up) scanned in 6710 seconds
```

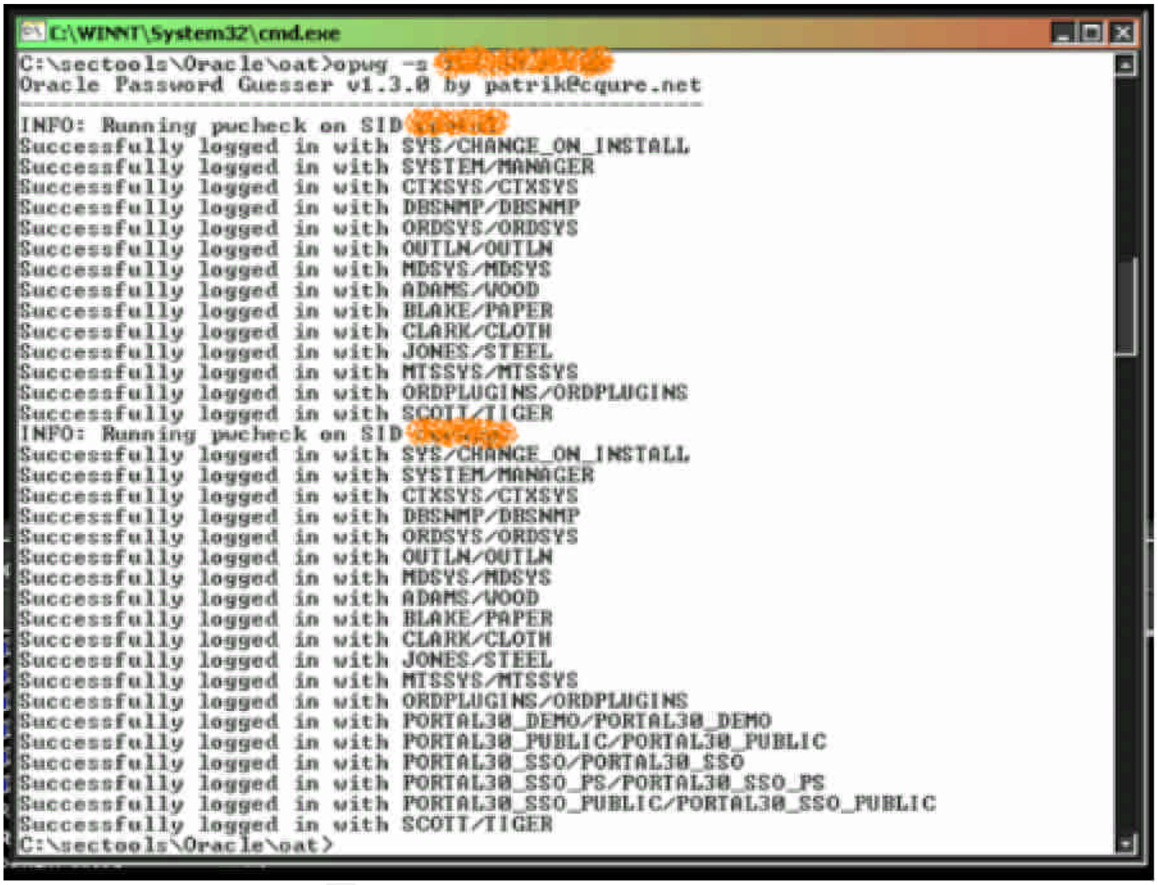
Step 3: Run Oracle Password Guesser

Each of the servers that NMapWin finds an open port 1521 can be tested for default Oracle passwords. In this case, the auditor is using SecuriTeam's Oracle Auditing Tool (OAT) utility called Oracle Password Guesser to determine if the current Oracle accounts and passwords have been secured.

To run the password guesser, open a command prompt, and change directories to the location where Oat was installed. Then, run Oracle Password Guesser with the following switches: >opwg –s 10.1.1.203.

Step 4: Analyze the Results

The application will connect to the IP Address that is placed after the –s in the command. The results of the test can be documented with a screenshot, or can be piped into a text file by adding "> Filename.txt" to the command line. This screen shot demonstrates what the feedback would look like from a server where the default accounts and passwords have not been changed.



```
C:\sectools\Oracle\oat>opwg -s [redacted]
Oracle Password Guesser v1.3.0 by patrik@cqure.net
--------------------------------------------------------------
INFO: Running pwcheck on SID [redacted]
Successfully logged in with SYS/CHANGE_ON_INSTALL
Successfully logged in with SYSTEM/MANAGER
Successfully logged in with CTXSYS/CTXSYS
Successfully logged in with DBSNMP/DBSNMP
Successfully logged in with ORDSYS/ORDSYS
Successfully logged in with OUTLN/OUTLN
Successfully logged in with MDSYS/MDSYS
Successfully logged in with ADAMS/WOOD
Successfully logged in with BLAKE/PAPER
Successfully logged in with CLARK/CLOTH
Successfully logged in with JONES/STEEL
Successfully logged in with MTSSYS/MTSSYS
Successfully logged in with ORDPLUGINS/ORDPLUGINS
Successfully logged in with SCOTT/TIGER
INFO: Running pwcheck on SID [redacted]
Successfully logged in with SYS/CHANGE_ON_INSTALL
Successfully logged in with SYSTEM/MANAGER
Successfully logged in with CTXSYS/CTXSYS
Successfully logged in with DBSNMP/DBSNMP
Successfully logged in with ORDSYS/ORDSYS
Successfully logged in with OUTLN/OUTLN
Successfully logged in with MDSYS/MDSYS
Successfully logged in with ADAMS/WOOD
Successfully logged in with BLAKE/PAPER
Successfully logged in with CLARK/CLOTH
Successfully logged in with JONES/STEEL
Successfully logged in with MTSSYS/MTSSYS
Successfully logged in with ORDPLUGINS/ORDPLUGINS
Successfully logged in with PORTAL30_DEMO/PORTAL30_DEMO
Successfully logged in with PORTAL30_PUBLIC/PORTAL30_PUBLIC
Successfully logged in with PORTAL30_SSO/PORTAL30_SSO
Successfully logged in with PORTAL30_SSO_PS/PORTAL30_SSO_PS
Successfully logged in with PORTAL30_SSO_PUBLIC/PORTAL30_SSO_PUBLIC
Successfully logged in with SCOTT/TIGER
C:\sectools\Oracle\oat>
```

Step 5: Pass or Fail

If any account and password combinations are returned after running the Oat utility, then the Oracle application has not passed verification. After disabling the accounts, or changing any weak passwords, it is imperative to rerun the Oat utility. This ensures that all of the accounts meet the password complexity requirements that are defined in LFO's password policy. In this example, 14 accounts are shown to have weak or default passwords. When no more accounts appear in the output, the application has passed. Because applications are constantly in use, and changes are frequently made to accounts and passwords, a security review process should be implemented to verify that the passwords remain complex. Additionally, a standard should be implemented so that any new Oracle installations are secured prior to being put online.

Audit Results for Item #2

In this case, all 47 Oracle servers on the internal network were found to have default accounts with default passwords. It was decided that all the Oracle servers be reviewed individually and have the accounts that are not needed disabled, and that the rest of the accounts should be given complex passwords that meet the LFO password policy standard.

Risk Analysis for Item #3 – Rogue Network Services

3.1. Threats and their Capacity to Inflict Damage

- **System** – Internal network
- **Vulnerabilities** –
  - Services that run on the network unnecessarily or unchecked can allow Trojans and malware to permeate the network
  - Potential overload of traffic may effectively cause a denial of service for network applications
- **Likelihood of Exploitation** – High
- **Value of the asset** – High
- **Potential Impact** – High
  - **Integrity** – Trojans and malware can delete or modify the contents of data on the network
  - **Availability** – Some Trojans cause Denial of Service attacks on the network as they propagate, causing servers to crash or become unavailable to process legitimate requests

3.2 Vulnerability and Impact for Risk

Item Number 3:
Are systems reviewed to identify and eliminate unnecessary services?

Risk:
NIST SP 800-26 defines the risk associated with unnecessary services by defining them as data integrity controls and stating: “Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity.”

Testing Procedure / Compliance Criteria:
Periodically scan servers to check for unnecessary ports or services.

3.3 Impact of vulnerability

Before a network can be managed properly, it is necessary for the engineers and administrators to be aware of what sort of services are commonly traversing the network. Becoming aware of what services are expected on the network is instrumental in eliminating whatever services do NOT belong on the network. Reducing network traffic to the smallest amount necessary will benefit everyone,

because with less traffic the network will perform better for the users, and the traffic will be easier to evaluate for the administrators.
One way to discover what traffic should be expected on the network is to determine what servers and services are needed for the organization. For example, LFO should expect to see Exchange traffic, because that is what they use for their e-mail services.

Servers and services that are not being used or that don't need to run can typically be discovered on most networks. Disabling these servers and services can free up valuable network resources. If LFO were to find peer-to-peer music sharing traffic on the network, it would probably not be considered appropriate traffic, and the network administrators would want to identify and remove the source of the traffic.

Being aware of what traffic is normal will alert network administrators to any new or unusual services that appear which could potentially harm the network.

3.4. List the primary vulnerabilities that could lead to the impact

Although removing unneeded services from the network can optimize the network by getting rid of unwanted traffic, another important reason to ascertain what services are running involves the discovery of Trojans and malware that could be running on the network unchecked. Trojans and worms use open ports and network shares to propagate. Locking down unused ports can help eliminate this risk, and protect network data. Trojans and worms can run on many ports, some of which are easily identified by their number like Back Orifice on port 54321. Other times, Trojans and worms conceal themselves by using well-known ports. Since it would be very difficult to identify a Trojan that is using FTP port 21, for example, administrators should strive to keep the number of servers that use FTP to the smallest number that is reasonably possible for their organization's needs. That way, if any FTP traffic started coming or going to a server that was not previously set up for FTP, the administrator's could investigate the system for potential malicious infection.

3.5. Scenario of exposure and means of exploitation for the vulnerability

In September of 2004, a worm called Win32.Dansh was discovered and assigned a "High" level of "Destructiveness" by analysts at Computer Associates. This particular worm had a payload that would modify a number of registry settings and would delete a group of .exe's. After making these changes to the system, the worm and its variants would then contact IRC servers and wait for commands. According to the Computer Associate's web page, some of these commands include:

- Start/stop/modify spread method and IP range
- SYN flood (Denial of Service)
- Start a Port scan
- Open a shell on an infected computer

- Download and execute files
- Uninstall the worm
- Execute files locally
- Initiate an FTP server
- Initiate a socks 4 proxy
- Initiate an HTTP proxy
- Obtain extended system information
- Connect to common ports on hosts to ensure they are open (including SMTP, FTP, TELNET, SSH and NETBIOS).
- Find open Telnet servers

Win32.Dansh variants also run a limited FTP server on a random port to provide a means for exploited machines to upload copies of the worm.

Adds User Permissions:
Later Win32.Dansh variants may also add a user *meandmyqwerty* to the infected computer to allow unrestricted access to the machine.

If LFO has no useful knowledge of what ports and services are commonly seen on the network, and if they happened to become infected with this worm, it would take valuable time for administrators to find out what is going on with their network servers. It is possible that the busy administrators would not even notice anything unusual on their network or servers at all. On the other hand, if the administrators had an optimized network, and were familiar with the exact number of FTP servers on the network, then would become apparent very quickly if this worm, Win32.Dansh, were to begin initiating proxy and FTP servers. Not only would there be an influx in the amount of traffic, but the IP addresses of the servers sending and receiving traffic would not be the IP addresses of the legitimate FTP servers. The new traffic would appear to be highly unusual, and the infected servers could be identified and dealt with in an appropriate and timely manner.

Testing for Item #3

Step 1: Use NMap to Find Open Ports

As demonstrated previously, Nmap is a utility that can be used to discover open ports on servers and help identify any rogue or unintentionally installed services. Though NMap is a straight-forward utility, it is also quite powerful, and can be used in a number of different ways. For example, a network administrator can use NMap to run a port scan to find ports associated with specific applications like FTP by scanning for open port 21. This would be helpful in identifying rogue servers or services that may have been installed unintentionally or with malice on the network.

Another scanning method that can be used involves running a full port scan, which scans for all open ports, either on a single server or on an entire subnet.

This second method of a full port scan is particularly helpful in finding backdoors and Trojans on the network.

In the output below, an Nmap scan identifies FTP services on the 192.168.76.x subnet. Because the auditor is looking for only FTP services for this particular scan, the "–p 21" switch is used to check each server on the subnet for an open port 21.

A more exhaustive scan can be run without designating a specific port. For example, the same syntax would be used as in the example, but would look like:

```
Nmap –v –sS –P0 –O 192.168.76.x > FTPScan.txt
```

The syntax is identical, but is missing the "–p 21" switch. Be prepared for a full port scan of a subnet or network to take a significant amount of time, depending on the size of the network.

Each live server on that subnet will respond with the status of port 21 (FTP). The status will be one of the following: open, closed, or filtered.

Step 2: Analyze the Results

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (192.168.76.0):
Port      State      Service
21/tcp   filtered    ftp
The 1 scanned port on  (192.168.76.1) is: closed
Interesting ports on  (192.168.76.2):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.3):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.4):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.5):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.6):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.7):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.8):
Port      State      Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.9):
Port      State      Service
```

```
21/tcp   filtered    ftp
The 1 scanned port on  (192.168.76.10) is: closed
Interesting ports on  (192.168.76.11):
Port       State       Service
21/tcp   filtered    ftp
Interesting ports on  (192.168.76.238):
Port       State       Service
21/tcp   open         ftp
Interesting ports on  (192.168.76.239):
Port       State       Service
21/tcp   open         ftp
Nmap run completed -- 256 IP addresses (256 hosts up) scanned in 6555 seconds
```

Step 3: Pass or Fail

Once the desired ports or services have been identified, a network diagram or other documentation will be crucial to compare services against. If no network documentation is available, a tedious process of identifying servers and appropriate services one-by-one will be necessary. If there are no undocumented or unnecessary ports open, then the network has passed.

If there are services that are running that have no documented reason for being active on the network, then the network has failed.

Once the scan has been completed, the resulting information can be used to create basic documentation. This documentation can be used as a comparison against future audits.

Audit Results for Item #3

Over the course of three weeks, complete port scans were run against all subnets at LFO, and a multitude of inappropriate ports, including FTP, were found to be open unnecessarily on the 277 servers. Two different Trojans were found to be using needless open ports to replicate themselves throughout the network. Because LFO does not use FTP internally for any documented business purpose, it was recommended that the ports be closed and FTP disabled on all internal servers. Although there are too many to list here, it was further recommended that all of the other open ports that were discovered, especially the known Trojans, be reviewed and investigated for appropriate use as well.

Summary:

LFO received a complete system audit against their internal network. The results of the audit provided valuable insight for the network administrators and assisted with the implementation of an enterprise-wide security overhaul that allowed them to become certified and accredited, and to meet their goal of being in compliance with FISMA requirements.

Although LFO had an appropriate security policy in place, it was determined that users were not taking it upon themselves to create complex passwords on their own. LFO took direct action as a result of the audit that showed how vulnerable the network was because of the common use of weak passwords. Because LFO was already in the process of implementing Windows 2000 Active Directory, they took the opportunity to implement strong password policy enforcement throughout the organization by using Active Directory Group Policy. Since password policies are set at the domain level of Active Directory, this ensures that all users logging into the Active Directory domain are in compliance with the password policy. Computers constantly become faster and more powerful, and new hacking and cracking utilities are always being published. No matter how much effort an organization puts into securing their environment, there will always be someone coming up with a way to compromise those efforts. Even though the passwords may meet the current complex password criteria, LFO should consider regular password assessments to verify that the complexity requirements continue to meet the organization's need for securing their network properly. By always being aware of the strength of their passwords, LFO will be empowered to make knowledgeable decisions about future security needs.

In the second audit, the accounts and passwords for the Oracle servers at LFO were checked for any default accounts that are installed by default. These accounts provide a method of access that the network administrators and Oracle developers were unaware of. Because of past problems with inappropriate activity on the Oracle servers, resulting in both financial loss and embarrassment for LFO, the security of these servers is considered to be a high priority for LFO. In this case the Value of the asset is very high. Due to past incidents, it is known that the Likelihood of Exploitation is also high. The result is a High Impact should the system be compromised. And because of past incidents, it is even more important for LFO that the problems are fixed because every further incident will harm LFO's reputation in exponential amounts. This audit revealed a basic security vulnerability on every Oracle server on the internal network. Of course, there were numerous other audits against the Oracle servers, including application scans and operating system vulnerability checks. However, the finding that the basic security measure of changing default accounts and passwords had never been instituted was a real eye-opener for executives and management in regard to how the Oracle servers were being administered. Within a week of receiving the audit results, a decision was made to hire a staff of Oracle database administrators to fill the knowledge gap between the Oracle developers and the network administrators who typically administered the servers.

The final audit point involves the discovery of services running on the internal network at LFO. A well known principal in the field of information security is "Know Thy System." When network administrators do not have the proper documentation of their network, they spend a lot of wasted time troubleshooting only the most important problems, a method known as "fire-fighting." When administrators spend their time fire-fighting problems on the network, the root of the problem is rarely ever determined, and problems are fixed with supposedly temporary solutions, known as “band-aids.” When this becomes common practice on a network, the network is out-of-control, and a new strategy for administering the network becomes necessary. In many cases, network administrators fall back onto fire-fighting and band-aiding because they don’t have the background information that they need regarding the current configuration of the network. Documentation is scarce and rarely up-to-date. Using a utility like NMap to document the network can provide the background information that the administrators need to gain an important understanding of how the network is put together. While reviewing the results of the NMap scan, a number of important questions can be raised or answered in regard to the network configuration. For example, administrators might find servers that are set up by different user groups that duplicate function. A clean sweep can begin on the network, and the documentation that results can lead to the implementation of a standardized method of installing and configuring servers, for example, because a complete discovery of servers and services can be compiled, maybe for the first time. In this case, the audit of network services was important not only because it enabled the beginning of valuable documentation and discovery, but because it unearthed two Trojans that were alive and well and living on the network. Prior to the audit, there had been no indication that anyone was aware of the infection. Once the Trojans were found, they were able to be eradicated.

As a result of the fact that LFO was required to be in compliance with FISMA standards, a complete audit was performed on their systems. Although the primary goal of the audit was to gain certification and accreditation, the audit helped open the eyes of everyone involved in the audit process. The audit did not just help them acquire their certification and accreditation, it also helped them gain valuable insight into the audit process, and more importantly, into their network configuration.

Works Cited:

Computer Security Division: Computer Security Resource Center (CSRC). Last updated: December 17, 2004. National Institute of Standards and Technology (NIST). November 4, 2004. <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

Default Passwords. 2004. CIRT.net. November 7, 2004. <http://www.cirt.net/cgi-bin/passwd.pl?method=showven&ven=Oracle>.

Large Federal Organization. *LFO Password Policy Document for Users.* Unpublished. 2003.

Virus Information Center. 2004. Computer Associates. November 7, 2004. <http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=40289>.

Appendix – LFO Password Policy Document for Users

Why do we use complex passwords at LFO?

As explained by the LFO IT Security Policy, security measures need to be in place to protect LFO's physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Well-chosen security rules and procedures do not exist for their own sake -- they are put in place to protecting important assets and thereby support the overall organizational mission.

LFO's IT Security Policy requires that all LFO systems be adequately protected by utilizing proper access controls, including the use of complex passwords. By requiring complex passwords to access resources on the network, LFO is ensuring due diligence to providing industry standard security measures, which will help prevent incidents of unauthorized access to sensitive network resources and data.

How am I identified and authenticated?

We are concerned about identifying you (identification) when you are working on one of LFO's systems, and your user identification (UserID) is used for that purpose.

Passwords are used to authenticate or prove that you are who you say you are when logging into our systems. Your password is something you, and only you, should know. Since you should always keep your password secret, when you use it, the system can trust that it is, in fact, you logging in.

The combination of you UserID and password uniquely identifies ad authenticates you to LFO's systems, and both should be carefully protected and never shared with others.

What do I need to know about password use in LFO?

- Use of passwords is required in LFO. Passwords provide access to LFO systems and resources for authorized users while denying access to unauthorized users.

- Your UserID and password identify you, and they must be protected to ensure no one can impersonate you. Don't share your UserID or your password with anyone. Do not write your password down; instead, create a password that you can remember.

- You must change your system password every 60 days. As a service to you, the system will notify you when it's time to change your password. If you do not change your password, you'll be locked out of the network until you contact the help desk to receive a new password.

- If your account is inactive for more than 35 days on any of our systems, your access will be revoked, and you will have to reestablish your account.

- You can't reuse your password for six iterations.

- Your password may not contain your userID or any part of your full name.

- Your password must be at least eight characters long and contain both characters and numbers. For stronger security, choose longer passwords with characters from all four classes.

- A complex password that cannot be broken is useless if you cannot remember it. For security to function, you must choose a password you can remember and yet is complex. For example, Msi5!YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).

- Your password must contain characters from at least 3 of the following 4 classes:

Classes	Examples
1. Upper Case Letters	A, B, C, … Z
2. Lower Case Letters	a, b, c, … z
3. Arabic Numerals	0, 1, 2, … 9
4. Non-alphanumeric ("special characters")	For example, punctuation, symbols. ({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=)

What happens if I forget my password?

You can try logging into an LFO system up to three times with different passwords; but, you account will be locked if you don't get in by the third try.

If this happens, you must call the Help Desk. The Help Desk will authenticate your identity. Once your identity is confirmed, the Help Desk will reactivate your account with a temporary password that must be changed the first time you use it to log in.