Global Information Assurance Certification Paper

Securing Real-World Systems
by
Security Auditing and Testing

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b

Option 2 – Case Study in Information Security

Todd Heath
SANS GSEC
December 10, 2004

Table of Contents

Introduction 3

Before Testing– Phase I 3

- System Information and Background 3
- System Test Plan and Procedures 4

During Testing– Phase II 4

- Analyze Findings 5
- Compare Findings 6

After Testing– Phase III 7

- Suggesting Solutions 8
- Reporting Solutions 9

System Maintainence – Phase IV 10

Conclusion 10

References 12

Introduction

In today's technological society it is not safe to release any unprotected information because someone that it is not directed may use it in a harmful manner. Thus, there has been major emphasis on Information Security otherwise known as, Information Assurance. The process of Information Security may be as simple as retrieving printouts so others may not view them or as complex as installing Intrusion Detection Systems (IDS) that will monitor all network traffic and notify the Information System Security Officer (ISSO) when there is unusual traffic possibly generated by a hacker. Marriam-Webster's dictionary defines a hacker as a person who illegally gains access to and sometimes tampers with information in a computer system.

Based on those assumptions, by reading this, one will gain the understanding of what is needed in order to properly secure a system and protect it from compromise. The example provided is a system that was under scrutiny for its password protection policy. The system will be measured against the United States Department of Defense (DoD) regulation as well as United States Army Regulation 25-2 (AR25-2). Sections that will be defined will provide insight on what should be accomplished will be the Before Testing stage, During Testing stage, the Testing Stage, and the System Maintenance stage.

Before Testing– Phase I

Before any testing may begin the security auditor must gather all the necessary information so he/she may know what the system's purpose is, its processes, and what type of information is transmitted. Since this system is being levied against DoD and US Army regulations this information is pertinent because depending if the system is classified or mission critical it will have to meet more requirements than an unclassified, or non-mission critical system. A mission-critical system can be interpreted as a system that if compromised, then may cause a loss of a mission or loss of life.

The system that will be analyzed will be an online education system; therefore the system will not be classified, but will contain sensitive user information. The sensitive user information will be the users Social Security Numbers (SSN). The use of SSNs enables the online university to track each user and their progress towards achieving a degree.

Most importantly it is important for the security tester it understand the System Information and Background, as well as, the tester must develop a Security Test Plan and Procedures during this stage.

System Information and Background

The system consists of a web-enabled application hosted at a common web facility with unique IP addresses, User IDs and Passwords. Connectivity to the website is provided by the hosting center and is connected to two major service provider networks with a total bandwidth capacity exceeding 10 GBPS.

The web sites are at a trusted facility and are protected by a router, custom firewall, and a switch with port routing to the web site. The system platforms run Microsoft Windows 2000 and uses a SQL database that provides querying, reporting

and analysis capabilities for the management of the system.

The network brings together a collaboration of colleges and universities offering a broad range of educational opportunities. The system currently offers approximately 15 programs from 8 different educational institutions. Through the system, the students have the opportunity to earn a certificate, associate, bachelor or master's degree from a home institution while taking courses from multiple colleges and universities.

The System Information is important to this process because the security tester must be aware of everything the system encompasses. This will allow the tester to gain an understanding of the hardware, software, and what ports and protocols are necessary for the system to function properly. Each system will operate under and assumed level of risk. Operating under assumed level of risk means if the system were to be completely locked down then it will somehow affect the systems functionality, and it will not operate as designed, therefore some risk must be assumed.

The specific requirement that is going to be tested is to see if the system is compliant with DoD 8500.2 and AR25-2 password requirements. The requirements will test the password's complexity and length. Other password requirements that the system must meet are password re-use, password expiration, and the systems configured lockout policy.

System Test Plan and Procedures

Based on the information provided in the System Information and Background the tester must begin to develop a test plan and procedures. The test plan and procedures should be given to the system administrators and any other persons that will be involved in the assessment of the system. The System Test Plan and Procedures state exactly each element of the system that will be tested and how they will be tested. There are manual and automated testing tools that may be used. In this security audit the following automated testing tools will be used:

- Harris Security Threat Avoidance Technology (STAT) Scanner
  - Developed by Harris Corporation, Harris STAT is a Common Criteria certified vulnerability assessment scanner that statically monitors a set of IT resources in order to identify configurations that may be indicative of potential vulnerabilities in, or misuse of, those IT resources.
- Microsoft Security Baseline Analyzer (MSBA)
  - MBSA is the free, best practices vulnerability assessment tool for the Microsoft platform. It is a tool designed for the IT Professional that helps with the assessment phase of an overall security management strategy.
- Defense Information Systems Agency (DISA) Gold Disk
  - Used to apply settings and vendor patches, validate and maintain compliance, and report system status.

Once all the testing plans and procedures have been outlined and delivered to the necessary persons involved, then the second phase – During Testing – is able to begin.

During Testing– Phase II

Now that the System Test Plan and Procedures have been developed and delivered to the necessary persons involved in the security audit the testing phase may begin. Again, it is imperative that the tester knows all information that is available about the system. An inexperienced or uneducated system security tester may cause harm to the system by making the system crash, potentially causing astronomical business loss for the system's owners. To avoid such a loss it is a good idea in the Before Testing Phase to try to acquire an identical system that is not in production. Some of the vulnerability testing tools that are being used have the ability to execute brute force attacks. Brute force attacks are attacks that attempt to gain access into the system and often times cause the system to crash or become inoperative. Therefore, if an identical non-production system is available it is in the system owner's and security tester's best interest to use the tools to assess the systems security. If there is no non-production system available for testing, then the Testing Phase should be done while the system is the least active. Again, this helps the system owner's in case something were to go wrong with any of the vulnerability tools which may cause harm. Also, by testing while the system is least active will make the Testing Phase quicker because the systems daily users are not taking up most of the resources needed to run the vulnerability tools.

Once the testing is ready to begin, one of the system administrators should be present or readily available in case the tester has any questions regarding the systems configurations. First, we ran Harris STAT vulnerability scanner that, depending on the scan type, STAT Scanner will check the password requirements and will also flag any vulnerabilities that exist. In this case, we ran a test that checked the password requirements, the ports and protocols that are being used, and whether any high-risk vulnerability exists.

After running Harris STAT Scanner and creating the necessary reports we are ready to run the MSBA vulnerability assessment tool. This tool also checks password requirements that are checked against DoD and Army requirements. MSBA also provides the tester the ability to check system patches and other configuration information that if not correct may lead to additional vulnerabilities.

Once the MSBA vulnerability assessment is complete and the reports are developed the DISA Gold Disk is used. The DISA Gold Disk checks for compliance with Information Assurance Vulnerability Alerts (IAVAs) that are issued by the DoD Computer Emergency Response Team (CERT), system patches, antivirus updates, and other system configuration that if not configured correctly may lead to vulnerabilities that may compromise the system's integrity.

Analyze Findings

Now that all the reports are developed from all three vulnerability scanners the tester now has to confirm if the results of the scans are correct. Sometimes vulnerability scanners tend to have false-positive and false-negative results. False-positive results are results that the scanners found as a vulnerability finding, but after further investigation are actually false. A false-negative finding is a finding that the scanners did not pick up, and upon further investigation the tester has uncovered that there actually is a finding. The reports that the security tester will analyze will be the technical results. Some of the technical results can be as detailed as the port

number, the port's purpose, the port's protocol that is being used, and any other information that may be pertinent to that port. It is important to understand the difference between the technical reports and the summary reports, which will provide output with less detail. Many times the system's owner is interested in the security posture of his or her system will not want to know the details. Also, upper management will not understand the technical terms and will just want to know if the system is secure or not, if not, they usually only are interested what do they have to do to secure it?

Compare Findings

In this particular case, we are only checking the password compliance. After further reviewing the results it is confirmed that the system administrators have kept compliance with all virus protection updates, DoD IAVAs, and have practiced good system maintenance by keeping up with all the current system patches and updates. By keeping compliant with all the current virus protection updates, DoD IAVAs, and system patches and updates the system is less susceptible to the known exploitations.

After examining that the system administrators have kept up with the most important updates it is time to see if they are compliant with the current DoD 8500.2 and AR 25-2 requirements. The following are the requirements for passwords that systems must meet according to DoD 8500.2:

- Password Complexity: Minimum of 8-characters, case sensitive, mix of upper case letters, lower case letters numbers, and special characters, including at least one of each (e.g., emPagd2!).
- Password Expiration: Enforce automatic expiration of passwords.
- Password History: Prevent password reuse.

Now that the requirements for DoD 8500.2 have been addressed the system must now meet United States Army Regulation, AR 25-2. The following are the password requirements for systems that must meet AR 25-2:

- Password Complexity: Minimum 10-characters long, minimum two (2) upper, minimum two (2) lower, minimum two (2) special characters (for example x$TloTBn2!).
- Password Expiration: Password expiration will not be more than 150 days.
- Password History: Password history configurations will prevent reutilization of the last 10 passwords when technically possible.
- Lockout Policy: Lockout policy should be set to 3 invalid logon attempts. Users will be locked out after 3 invalid logon attempts.

The system that was tested provided the following results in the vulnerability scans and password policy configurations:

- Password Complexity: 5-character, mix of upper and lower case letters.
- Password Expiration: Password expiration is set to 180 days.
- Password History: Remember last 3 passwords.
- Lockout Policy: Users are locked out after 5 invalid logon attempts.

The following table is generated to allow a cross section comparison between the

two regulations and the system security configuration at question.

	DoD 8500.2	AR 25-2	System Security Configuration
Password Complexity	Minimum of 8-characters, case sensitive, mix of upper case letters, lower case letters numbers, and special characters, including at least one of each (e.g., emPagd2!).	Minimum 10-characters long, minimum two (2) upper, minimum two (2) lower, minimum two (2) special characters (for example x$TloTBn2!).	5-character, mix of upper and lower case letters.
Password Expiration	Enforce automatic expiration of passwords.	Password expiration will not be more than 150 days.	Password expiration is set to 90 days.
Password History	Enforce automatic expiration of passwords.	Password history configurations will prevent reutilization of the last 10 passwords when technically possible.	Remember last 3 passwords.
Lockout Policy	Lockout policy should be set to 3 invalid logon attempts. Users will be locked out after 3 invalid logon attempts.	Lockout policy should be set to 3 invalid logon attempts. Users will be locked out after 3 invalid logon attempts.	Users are locked out after 5 invalid logon attempts.

The table above allows anyone that is interested in the current security posture of the system to get a quick pulse check to see where the system stands. This table could also be of some use to the After Testing phase where the reporting comes in.

After Testing– Phase III

In the first two phases the security tester gathered the required information, ran the necessary tests, and created a way to compare the results against the requirements, now we can begin to further analyze the results and provide the system's owner with necessary actions to mitigate the findings.

Judging by the table created above, it is easy to see that the system under scrutiny only meets one of the four requirements: Password Expiration. Having said that, it does not necessarily mean that the system is susceptible to any malicious attacks, because the system administrators have kept a good eye on every system patch, IAVA, and virus protection update that has come out. After manually verifying the scan results that yielded that conclusion, it is safe to say that this system is fairly secure, but does not employ best security practices.

How GSEC Affected Me in Suggesting Solutions

After learning a great deal from my SANS GIAC Security Essentials Certification

(GSEC) about Information Security finding a solution for this client was not hard at all. The GSEC study information allowed me to obtain the necessary knowledge on why these aspects of password compliance should be strictly adhered to.
I learned that the Password Complexity and Lockout Policy go hand-in-hand. Users should set a password that is not easy to guess, exemplifying why the regulations require at least a case sensitive 8-character, mix of upper and lower case letters, and special characters. This will keep the user from creating a password that would be easy to guess, for example, the users Social Security Number (SSN), address, birth date, etc. The reason that Password Complexity and Lockout Policy go hand-in-hand is because if a malicious attacker were to attempt to crack the complex password created by the user and failed three times, the user would be locked out. This would alert the user that someone was trying to login maliciously. Along with alerting the user, most system administrators have their systems designed for when a user is locked out an audit log is created, where they can gather information and try to track down the malicious user.
Along with the previously discussed aspects of Password Compliance, Password Expiration and Password History are equally as important and should not be overlooked. The GSEC study material allowed me to understand that my expiring the users password, while sometimes frustrating for the user due to the complexity of the password, make the users passwords that much harder to guess. Again, adding to the users frustration by not allowing them to use a previously assigned password is also a good security practice that should be used. This will also not allow password repetitiveness, thus increasing the information security.

As previously mentioned, many users that do not understand the importance of information security find many of the password policy measures very frustrating and try to find ways around them. As John O'Leary states in his article, *How to Create and Sustain a Quality Security Awareness Program,* "The most serious and potentially damaging IT security-related acts are almost always done by those with some form of authorized access. Employee attitudes and motivations must be a critical concern of all IT security programs". Therefore, it is to the utmost importance that any organization should educate their users about information security and allow them to realize that these measures that have been put in place are there to protect them and the organization as a whole. Through this education process the users should learn that they are not to create an easily guessed password. Among many other restrictions users should be urged not to write down their password and keep it close for them so they can remember it. The password should be committed to memory as quickly as possible because if they kept the password on a note and it fell into the wrong hands the whole organization is at stake.

Suggesting Solutions

When suggesting solutions one should always keep in mind, how are the solutions going to affect the system? Will they affect the systems users, daily activities, the system's purpose or mission? Another factor to take into account is how complex the solutions are to implement. Having learned from my GSEC studies, the password policies that have been analyzed can easily be changed without having much impact on the system. Many times I have encountered a client that has had an unsecured system, but has invested a lot of money in the system thus far. Such

clients are very reluctant to implement security changes because of the cost that may be associated with the change. They often only see the monetary value and not the risk that is associated with the risks that have been identified.

Keeping those questions in mind, the following suggestions have been made for this system to become password compliant with DoD 8500.2 and AR 25-2. First, the system should comply and meet the AR 25-2 minimum 10-character password requirement. By implementing this requirement the users will now be required to make a more complex password, which will be much harder for a malicious individual to guess the password. This solution is very easy to implement and should have no affect on the system's functionality or mission. Secondly, the Password History should also become compliant to the AR 25-2 minimum of remembering the last 10 passwords created. Again, this will be fairly easy to implement and will mitigate this finding. Finally, the system should meet the Lockout Policy requirement, which is, after three invalid login attempts the user is locked out for a period of time. Another security feature that is suggested is when a user is locked out, to create an audit log and keep them on file. This will help the system administrators in identifying any unauthorized attempts into the system.

By implementing the above suggestions the overall system security posture has been greatly improved. The system before security testing was implementing the correct system updates and other major updates, but sometimes the simplest security feature that is not implemented correct can leave an open hole where an unauthorized user may gain entry. Again, the above suggestions may make the system's users somewhat frustrated and that is why I suggest that before implementing the correct password policies that every user understands why such restrictions are being implemented. Once the users realize that it is only there to further protect them, most, if not all, will embrace the change.

Reporting Solutions

Now that the solutions have been selected and justified, it is time to report the solutions to the necessary persons. When reporting the solutions the security auditor must been aware of his or her audience that they are reporting to. Therefore, many different types of reports have to be developed. As previously mentioned the upper management that are interested in the results of the security testing efforts are only interested in what has to be done to fix the findings. This type of report will mainly contain the following:

- Number of findings listed by severity
- The finding(s) severity
- If it is possible to mitigate the vulnerability in a timely manner, or if it will take time and money to mitigate the risk.

The details of how to fix the findings will most likely be left out because the upper management may not have the expertise needed to fix the problem.

The other reports that will be generated are the technical reports. These reports will contain detailed information about each finding. The level of detail that these reports will contain will usually be following:

- Number of findings listed by severity
- The finding(s) severity
- Detailed information about the vulnerability, the harm that it may cause, and how

it can be exploited
- Detailed step-by-step directions on how to mitigate the risk associated with the vulnerability

It is necessary to always provide the system owner's and system administrators with the correct information and debrief them on what took place and discuss all the findings. Many times if some high-risk vulnerabilities are discovered it is necessary to walk the system administrators through the problem, so they will understand the seriousness of the risk and how the vulnerability could be exploited. Many times it will be necessary to re-test and complete Phases I-III to ensure that the vulnerabilities that have been found have actually been mitigated and the system is no longer at the risk that you defined. Once the system's vulnerabilities have been mitigated the risk level of daily operation will be brought down from a high or medium risk of exposure to a low risk of system compromise. When this is done, it is now necessary to move onto Phase IV.

System Maintainence – Phase IV

Now that the solution to the identified vulnerabilities have been corrected and implemented many system owners and administrators tend to forget the whole purpose in the security audit and testing. The purpose of the security audit and testing is to identify and mitigate any vulnerability that could compromise the system. I have seen this problem time and time again in information security. Sometimes information security is seen as something that is in the way of getting the system approved for use, where information security is keeping the system up and running.

I feel that each Phase in this audit is extremely important, but I feel that a great amount of emphasis should be placed on this last phase. The reason more emphasis should be placed on Phase IV is because after many systems go through Phase I-III, Phase IV is often overlooked. In this last phase the overall system security integrity should be maintained. This includes keeping compliant with the necessary regulations as they are approved. Vulnerabilities are uncovered regularly; therefore if the system is not updated on a regular basis the system may become subject to compromise.

One policy that I suggest to many system owners and system administrators is to create an organizational policy of their own. Many Government organizations employ this method, for example, Dan Caterinicchia mentioned in his article, *"Army Adds Depth to net security"*, that the Army gives a 90 day deadline to respond to any IAVA release. This policy should outline a certain timeframe that the system administrators have to implement a major system patch or update. I also suggest that, if possible, virus definitions be updated the same day they are available and to run weekly virus scans on their systems to ensure the system remains healthy.

Conclusion

Information Security is an aspect in Information Technology that has developed to be a major role player throughout the industry. Many businesses and organizations have begun to take many of their operations online and wish to protect all their assets while doing so. An integral part of protecting assets online is securing the computers and networks that enable them to make their information readily available is security

auditing and testing.

As mentioned before, the four phases of security testing, Before Testing – Phase I, During Testing – Phase II, Post Testing – III, and Phase IV – System Maintenance.

Each of the first three phases is as equally important in successfully securing any system or network. The fourth phase – System Maintenance will help ensure that the system or network that has been secure and runs on a low-risk level will stay that way.

The solutions that were developed to help the system mentioned were used and after implemented. Before finalizing the implementation of the new password policies the system administrators tested the system to ensure that the new policies invoked did not affect its functionality. I now use the four-phase process in each system security audit and system security testing. The four processes allow me to gather information about the system, test the system, analyze the results, and provide feedback that is in the best interest to the system owner's.

References

Caterinicchia, Dan. "Army Adds Depth to net security" FCW.COM. 2004. April 29, 2002. <http://www.fcw.com/fcw/articles/2002/0429/tec-scan-04-29-02.asp>

Harris Security Threat Avoidance Technology (STAT). 2004. December 17, 2004. <http://www.stat.harris.com/index.asp>

Jackson, William. "NIST and NSA draft safe-IT profiles" Government Computer News. March 10, 2003. <http://www.gcn.com/22_5/tech-report/21312-1.html>

Joint Task Force – Global Network Operations (JTF-GNO) Home Page. 2004. December 15, 2004 <http://www.cert.mil>

Microsoft Baseline Security Analyzer. 2004. December 11, 2004. <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

O'Leary, John. "How to Create and Sustain a Quality Security Awareness Program" Computer Security Institute. 2004. <http://www.gocsi.com/training/erc/hcsqsap.jhtml>

United States. United States Army Regulation. Information Management: Management of Subdiciplines. Information Assurance. Number AR25-2. Washington: November 14, 2003.

United States. Department of Defense Instruction. Information Assurance (IA) Implementation. Number 8500.2. Washington: February 6, 2003.