Network Security Audit

D.Liu and B.V.Ghita

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

With the increase of broadband connections users, the number of home computers has increased importantly. As a consequence security issues have gained in importance in this domain. Most of these new computer users are novice and do not have the knowledge to understand exactly the repercussion of their actions in term of security on their machines. Software companies have developed several products to protect these stand alone computers. Some of them are designed to produce security audits which evaluate the security risk of the Personal Computer (PC).

Unfortunately, even with these audit programs, users do not become aware of the danger they can face on Internet. This project has developed a security audit tool which is intended for novice computer users. This tool's objective is to evaluate the materiel security level and the behaviour security risk of the user. Moreover, to be sure of the users' understanding, this tool also contains some explanation and demonstration elements, which show them how a malicious person can exploit their lack of prudence.

Keywords

Security, Audit, Ports, Novice users, Key logger, Password, Antivirus.

1. Introduction

Security has become a critical issue for modern companies, they are actually spending important amount of money to prevent any malicious persons to access their data. With this increasing level of protection, hackers are turning away from banking and high technology companies, and are more targeted into small organisations or ordinary single PC/home networks which are less secure.

Aware of this, software producers have developed very efficient products adapted to ordinary Internet home users like personal firewalls and personal antivirus. Unfortunately on the other hand their use generates a wrong feeling of security. Most of time, these tools are not configured properly by users, who do not have the right knowledge. In this case the computer is still unsecured.

In this project, the author is going to try to make them understand the risks they can face on Internet network by using simple demonstrations and explanations,

First of all, a software application should be built to execute technical tests of the computer and produce a physical security audit. To be able to provide external and

internal tests, the application will have a client server configuration. The server side of the application will be put online, and will execute external tests and attacks. The client part of the application will be run on the local host and will offer local tests possibilities.
This program must be as easy as possible to use in order to make it accessible for every ordinary computer user. Unfortunately a technical audit is not enough to evaluate the security level of a computer, human behaviour is also a key element. To assess the user, a MCQ will be integrated to the software application. In this questionnaire some questions will focus on the existing security element of the PC, and some others will deal with the user's behaviour in front of different events: for instance a website which asks the user to download and execute a JavaScript program.

Combined with the technical audit results, the user will be able to have a very accurate and customised security audit based on both the machine security configuration and the user behaviour. Moreover, to provide a better understanding of the MCQ questions, they will be illustrated by screenshots and schemas.

Once the audit results have been given, the application will be able to help the user to understand them. It is important to keep in mind that ordinary PC users have really few knowledge to exploit theses results. For the third part of the project, some informative pages have be included and linked to the audit results to provide explanation and give advices to the users to avoid problems which have been detected.

2. Existing audit software

Before starting the conception of this project's audit software, it is important to have an overview of existing audit tools used by network administrators. Here can be found the analysis of four of them.

2.1 Nessus

It is maybe the most famous one. It is a free vulnerability scanner based on client-server architecture. Normally it runs on UNIX like systems, but recently a windows version has been adapted: Tenable NeWT Security Scanner (Nessus, 2005). It is this version tested. The functionality of Nessus is very similar to the audit tool this project should produce. The client part of Nessus allows the interaction between the user and the machine, by sending to the server the user's instructions. The server receives the user's information, then runs the appropriate command (attack test) and finally sends the result to the user. This program has three main positive points: first of all, it is free; secondly, it is coded as a plug-in, making him easy to update; and at last, it contains a wide range of options to parameter the vulnerability audit.

2.2 ATK: attack tool kit

It is also a free audit software, it is based on a mix between a vulnerability scanner and a exploiting frameworks (ATK, 2005). This application has two main benefits:

firstly it is very easy to exploit and uses schemas representations to explain to users its functionality; secondly, it provides advices to avoid the security hole if vulnerability has been discovered.

2.3 GFI LAN scanner

It is a complete security software. Once launched, it will perform an external vulnerability scan and also an internal security audit (GFI, 2005). This internal security scan will check in the current computer or on every host of the LAN (Local Area Network) the installed softwares, their patches, the passwords used, the USB connections, the register entries, the shared folders, the wireless access points, etc…

2.4 MBSA (Microsoft Baseline Security Analyser)

It is a security tool created by Microsoft for Windows based computers. "It scans for common misconfigurations in the operating system, IIS, SQL, and desktop applications, and can check for missing security updates for Windows, Internet Explorer, Windows Media Player[…]" (Microsoft, 2005). MBSA is directly connected to the Microsoft Vulnerability database, which gives him the advantage to be constantly up to date. Moreover, it provides to users clear explanations and solutions to discovered problems.

3. Important Issues

All security risks and protection elements are well known from professional security administrators, but on the other side, ordinary people can have some problems to understand them. Even if they use a familial version of security audit software, they may not be able to interpret its results.

Software designers try to make their product as simple as possible to affect as many users as possible; but unfortunately, because of the complexity of the network security area, it is very difficult to create something really comprehensible for any ordinary user. For instance, with Nessus even an intermediate knowledge level user will need about ten minutes to realise all the possibilities of this program and how to exploit it efficiently.

Moreover today's security audit programs can be very complete from a technical point of view. Unfortunately they do not take into account the human behaviour factor which is the weakest link in the network security chain.

The last issue of this project which makes it different from other commercial audit softwares concerns the usage because all existing softwares need to be installed on the computer they are auditing. This obligation can be a serious problem for very novice computer user who do not know how to install, or for users who do not have an administrator account on the current computer or who do not have the right to install any programs on it.

This project tries to offer appropriate solutions to these issues. Firstly, it will not require any installation obligation. Thus it will provide to any users no matter the computing knowledge level the possibility to run easily a security audit on the current computer. Secondly on top of all technical audit elements, this project will contain some tools which will evaluate the security level of users' human behaviour. Finally, the users' understanding is a key element in this project, they will be provided clear explanations about how to use the different audit elements, what are they auditing, how to avoid the problems….

4. The audit programs of the project

After the study of exiting audit programs, some audit tools have been chosen to be integrated in this project. They can be grouped into two categories, the ones which analyse the material security risk and the ones dealing with the human behaviour risk.

4.1 Material audit elements

4.1.1 The port scanner

It is based on a client/server architecture. The client is launched from the audit web page on the user's computer and then sends a request to an external server which will scan the current PC's ports. The user will be given the choice between a "quick" scan and a "long" scan It has been decided to add this option because a complete port (long scan) scan takes about 20 minutes, and it is not possible to impose a time consuming test. The "quick" scan takes about 30 seconds, and it checks 31 "well-known" ports. Once the user has clicked on the start button of the user interface, the client program will be run; it will send a scanning request to the server. Then, the server will analyse the request, find out the IP address of the user from the connection settings and finally run the appropriate IP scanning program. There are actually two scanning programs, one for each type of scan (quick and long), but their functioning principle is the same. They try to create a socket connection with the given port in a specific timeout. If this try fails that would mean the port is closed, inversely if it success it would mean that the port is opened. For the "well-known" ports scanning, the timeout is set to one second, and for the complete one, it is set to 200 milliseconds. The longer is the timeout, the more it can be certain that the port is closed. To scan 65535 ports, it is not possible to set important timeout; otherwise the scanning process will take hours.

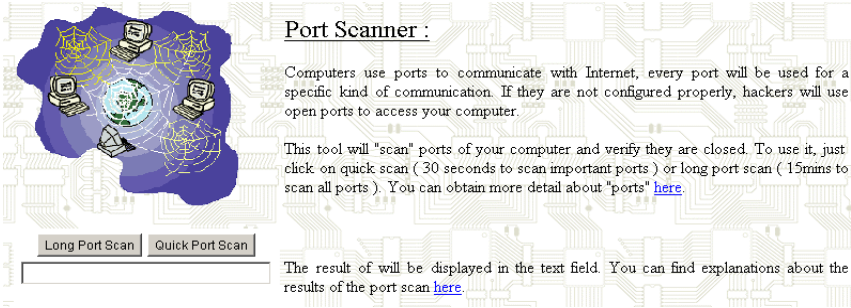

Figure 1: the port scan interface, with a scan result displayed.

The scanning result is recorded in a table and transferred to the server who will convert it into a single data flux and send it back to the client program. Once the client has received the result it will display it in the user interface of the audit page.

4.1.2 The Antivirus tester

It will analyse the reactivity of the antivirus installed on the machine. Recently some online antivirus have been developed, they can perform a complete hard disk scan of people who connect to their WebPages. But they do not perform real tests which can audit the reactivity of the installed antivirus. To test the reactivity of user's antivirus; the project uses elements of EUCAR virus test file. "This test file has been provided to EUCAR for distribution as the EUCAR Standard Anti-Virus Test File", […]. It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (though they typically report it with an obvious name, such as "EICAR-AV-Test")" (EUCAR, 2004). The tester creates an "eicar.exe" file on the disk on the user's machine then copies the following 68 bytes ASCII characters in it: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*.

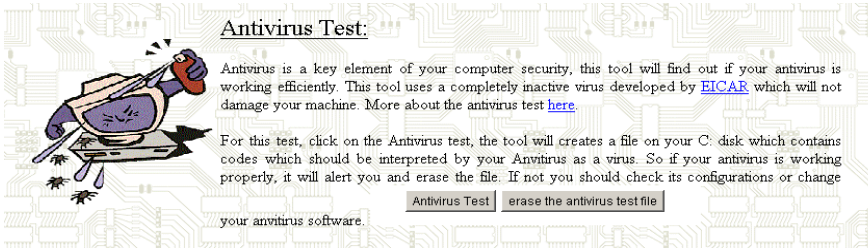

Figure 2: the user interface of the antivirus test tool.

Normally, the antivirus should alert the user that an infected file has been detected. If nothing happens, that would mean that the antivirus is not properly configured or not efficient. Finally the tool will give to the user the possibility to delete the file.

4.2 Human behaviour assessment tools

4.2.1 The password analyser

Depending on the password entered by the user, the analyser will estimate the amount of time needed to crack it. There are several free password crackers which can be used to show to users how easy it is to crack a weak password. But their main defect is the delay required to crack it. If the password is not a dictionary word, it may take from a few minutes to hours to break it, and users can not wait so long. So instead of integrating one of them, the author has decided to develop a time estimator which gives a quicker response.

The user is asked to enter a password, and then the tool import a list of English dictionary words from a specific webpage (http://dcool75.free.fr/mot.txt). Once the list is imported, it will compare the user's password with its content. If there is a match, it will inform the user that only a few seconds are required to crack this password.

If there is no match, the audit tool will process to the structure analysis of the password; depending on characters it is built with; the program will calculate an estimation of time needed to crack it with any ordinary password crackers.

This estimation is based on the password's length, and the type of characters it contains. Basically, if the user's password contains capital letters, numbers, and special characters, it would take approximately 4320 minutes to find out one character. If it contains only lower case characters, the cracker will need about 4 minutes per character. If it has some number on it, 30 minutes are required for each character. And finally if it contains numbers and upper case characters, it will take about 150mins to find out a character. These numbers come from statistics the author has done with L0phtcrack 5.04 a very popular password cracker.

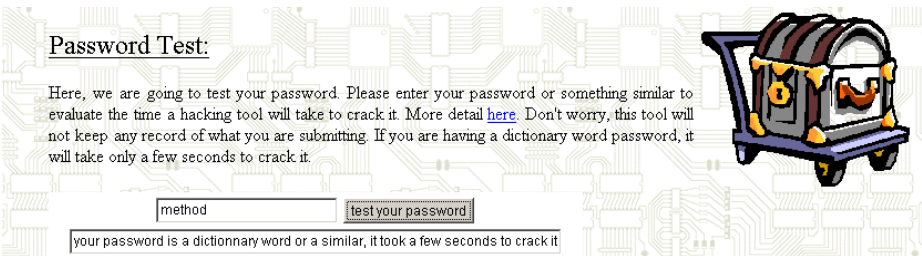

Figure 3: the result of the password tester when the password is a dictionary word.

4.2.2 The MCQ

Here the users have to answer some questions about their behaviour when they meet some specific situations. Most of the existing security audit softwares do not take into account the effects of human aspect on the security. Here depending on the

users' answers, a specific amount of points will be added to the risk counter. Once all questions have answered, the final risk counter will determine in which category the user belongs to: low security risk, medium risk, high and very high risk.

4.2.3 The key logger

It is more a demonstration tool than an auditing tool. It is important to show to users how a real hacking tool works. So they will realise by themselves how dramatic it could be if a hacking tool of this kind was installed on their computer. In order to avoid any installation requirement to use it, it has been preferred a simple design with an easy usage instead of complex codes similar to commercial key loggers which would require manipulation from the users. So the program included into the audit page has nothing to do with a real key logger except the concept. It does not run in the background of the computer to capture every keystroke but clearly asks the user to write a few words in a designed square of the audit page. When the user has written 10 characters the JAVA program will create a socket connection with the key logger server, and everything that is in this square will be sent then, the server will process the data. Here to give a quick demonstration to the user, the server will send the data back to the audit page which will display it in a pop up page.

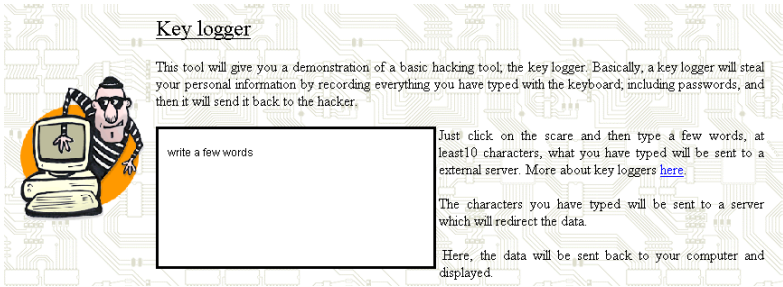

Figure 4: the interface of the key logger where the user is invited to write a few words in the indicated area.

5. Achievement

The final security audit program of this project has been integrated in an online web page (http://dcool75.free.fr), when existing audit softwares require an installation on the computer it is testing. So the accessibility is far simpler, the users have just to go to this page in order to test the security of their computers.

Another good point of this project is that it has been designed to be used by very novice users. When existing audit softwares perform only their tests and provide a final result, this project's program gives clear explanations about the audits elements, why they have been chosen, how they are functioning, how to exploit the results and what are the security risks.

The last important difference of this security audit project with other programs is that it is commercially neutral. An important part of existing audit programs are designed by security software companies, and sometimes they try to make the audit result

worse to encourage people to buy their products. It is frequent to see in an audit result: “Your computer has a very high security risk, if you want to fix the problem buy the following products of our company”.

Here, the audit project has no commercial purpose and always advice the users to download freeware security programs.

6. The survey

A survey has been added in the main audit page, in order to collect users’ opinions about this project and its programs. It does not contain a huge number of questions, but it will give the possibility to know if this project has reached its main objectives. In addition, it will provide a very interesting comparison from the user point of view of this audit program with commercial security audit softwares.

A part of the novices users questioned had not fully exploited the audit programs which compose this project. After investigations, it turns out that some of them had a firewall which blocks the client/server communication of the port scanner and key logger; and others did not have properly modify the JAVA security policy on their computer. That means that the project has only reached partially one of its main aims which is to create an audit project accessible to everybody.

The general opinion of users is that they really appreciated some elements they consider to be real innovations. The antivirus tester and the password analyser for instance were real success, similar tool do exist but they all require installations in order to be run.

A new problem has also been raised by this survey. Some users explained that the manipulations required to change manually the JAVA security policy may discourage novice users. To modify a security file on the hard disk of the computer because a web page says so is not something every user will do. Most of users will certainly be afraid of this step because their do not know the origin of the web page, and it they are novice users they will not know exactly what they are doing. That is why it is a key element in future improvements to bypass this step by using another coding language which can be less strict in terms of security or by developing some script which will make the modifications of the policy file automatically each time the audit page is loaded by the web browser and will erase the modifications once the user has closed the page.

Additionally the analysis of expert and intermediary users’ answers has proved that they were able to use the audit programs without any technical problem. Most of them have found this project simple to understand and easy to use comparing to existing security audit softwares. Thus, it is reasonable to say that this project is more interesting than existing audit softwares in terms of usage simplicity, but some improvements are still required to improve the understanding of novice users.

7. Conclusion

By studying some existing security audit programs, this research has identified some key issues which could be improved for very novice computer users in terms of understanding and manipulations.

This project has developed an online webpage which contains a set of security audit tools and clear explanations texts. This project brings to novice users a simpler overview of their computers' security via technical audits and human behaviour assessment. Moreover this research gives to the end users the possibility to have a better understanding in the domain of computer security thanks to its explanations texts which describe in detail each security element broached in audit the webpage.

In order to make this project technically more complete and competitive with existing commercial audit programs in the future, some new audit programs can be added. For instance, inspiring from Microsoft Baseline Security Analyser, an upgrade analyser can be added to the project. It would analyse the upgrade level of the Microsoft products: Microsoft Windows, Microsoft office, Microsoft Internet explorer; with the latest version published by the Microsoft web site.

8. References

ATK: Attack Tool Kit, (2005), http://www.computec.ch/projekte/atk/, accessed in September 2005

Eucar Online, (2003), *The Anti-Virus Test File*, www.eicar.org/anti_virus_test_file.htm#dl, (accessed in August 2005)

GFI, (2005), http://www.gfi.com/lannetscan/ accessed in September 2005

Microsoft, (2005), http://www.microsoft.com/technet/security/tools/mbsahome.mspx, (accessed in March 2005)

Nessus, (2005), www.nessus.com/about/, accessed in September 2005.