

**Computer Security**

**Tutorial 7: What does your computer say about you?**

*As with all applications, there is always the possibility of the software potentially causing harm to your computer. As a result, you should always scan any downloaded files and software using an up-to-date anti-virus product. Furthermore, you should test and examine security software on an isolated computer which will not damage any local files, or any other computers which are connected to it. Lastly, by continuing with this activity you will not use any of the tools for malicious or destructive purposes.*

In many instances, end-users are quite often unaware of what information their computer holds about them. In this tutorial you will learn that there are many freely available, and easily accessible tools which can be used to acquire private information about an end-user through the data residing on their computer.

**Part 1: WinAudit**

The first security tool which we will explore is WinAudit. WinAudit is a freeware (self contained) product, designed to allow individuals to audit a Microsoft Windows based computer. You may obtain WinAudit from <http://winaudit.zymichost.com/index.html> or from Blackboard directly. You should scan the file prior to executing it to ensure that it is safe.

Once the correct file has been extracted from the compressed folder, WinAudit can be run by double clicking the executable file. This will automatically load and display a window similar to what has been presented below.

The first step is to allow the program to audit your computer. This can be undertaken by click the “To audit your computer click here” button. The process should take no more than a couple of minutes to complete.

You will see that a series of *categories* are created once the software processes your action. By clicking through the various categories you will see that in just a couple of minutes the application has extracted a wealth of information regarding the current state of your computer. Spend a few minutes ‘auditing’ your own computer, paying special attention to the *security* category.

1. Imagine that the software was executed and run remotely. The attacker now has access to a wealth of information regarding the state of your computer. How would this information be used to further compromise your computer?
2. How could each of the aims of security (confidentiality, integrity and availability) be compromised through the (WinAudit) information available to you?

**Part 2: PC-Time**

The next security tool which we will briefly experiment with is called PC-Time. PC-Time is a self-contained freeware software, permitting you to monitor when and for how long any computer has been used for during any given time period. A compressed zip file has been placed on Blackboard under this module. To run the program, simply double click on the executable file and view the reported information of the program.

1. Why would knowing when and for how long a computer was used be beneficial to an investigator who is auditing a computer?
2. In the full version of the software, the investigator may use the software to view the usage time of other computers on the network. How would this information be beneficial within a place of work?
3. Try to come up with three other scenarios in which such a tool benefit an investigator, OR an end-user?

**Part 3: MyLastSearch**

MyLastSearch is a freely available tool allowing you to view the search history of your web browser. You may download a copy from [http://www.nirsoft.net/utils/my\_last\_search.html](http://www.nirsoft.net/utils/my_last_search.html%20) or obtain the software from this week’s module on Blackboard. Once you have downloaded and extracted the software, simply double click on the executable file to run the program. The program will immediately collect, interpret and present your search history for the computer you are currently using.

1. What privacy concerns exist with using a program such as MyLastSearch?
2. How could this software be misused if it were used by someone who had temporary (and unauthorized) access to your computer?

**Part 4: IEHistoryView**

IEHistoryView is a freely available tool allowing you to view all the websites which have been accessed via the computer that you are currently using. You may download a copy from

http://www.nirsoft.net/utils/iehv.html or obtain the software from this week’s module on Blackboard. Once you have downloaded and extracted the software, simply double click on the executable file to run the program. The program will immediately collect, interpret and present your search history for the computer you are currently using.

1. What privacy concerns exist with using a program such as IEHistoryView?
2. An individual could potentially deny accessing one or all of the websites listed in the IEHistoryView window. What data does IEHistoryView also present which could distinguish an ‘accidental’ accessing of a URL versus an intentional continuous access of a specific URL?
3. How is IEHistoryView different from MyLastSearch? (You may need to go back and run MyLastSearch to compare the result).

**Part 5: Metadata**

Often end-users will leave confidential and/or private information within documents. As a result this information could be utilised to determine the owner of the document. Download and open the document titled ‘Fictional Press Release’ from Blackboard. As the name suggests this is a press release outlining new products from a fictional company. Upon initial examination the document seems harmless. However it contains a wealth of information that the company would probably not want released. How much of this information can you find? What other ways can you think of in which data might accidently be leaked when making documents public?

**Part 6: Question**

Australia Post has just delivered your international passport which contains an RFID tag containing your sensitive information. A week later while shopping, you notice a salesperson selling a protective cover for your passport. The salesperson's solution costs $79.95 and protects your passport from being read via radio waves while it is in your pocket. Explain how you could achieve the same outcome for under $5.00.