Remediation Through Best Practices

This tutorial explains many of the practical steps you can take to protect a Windows based computer from trivial exploitation.

The steps covered in this tutorial do not need to be performed in any particular order, but they should be repeated regularly (monthly, quarterly...) because computer system change frequently and often without your being aware. For example, an update from a software vendor can silently open a new port for the first time exposing you to attack. An update may also reset any default user accounts and passwords to their factor defaults without your being notified.

The steps we will look at include; anti-virus protection, open ports, out-dated software, vulnerabilities, and default passwords.

Anti-virus protection

First of all, make sure you have an anti-virus program running, properly configured, and up-to-date. Typically, there is the actual virus scanning program along with frequently updated virus identification files.

Proper configuration includes;

- enable automatic updates of virus identification files
- enable automatic full scan
- enable scanning archive files, email, removable media, web pages, and downloaded files.

Open ports

Practically all network communications between computers involves IP addresses and ports. Imagine an apartment building. The apartment building is the IP address, it is enough to get you to the correct computer. However, we typically have several programs running that are all communicating across a network. Each program on a computer that needs to communicates across a network is assigned a port number to uniquely identify that program. This is why you can have an email program and web browser running at the same time and you do not get email and web pages show up in the wrong screen.

So while the apartment building is like the IP address, the apartment numbers are like the port numbers that identify each distinct apartment/program.

There can be up to 65,535 TCP ports on one computer alone. Each representing a running program that can both respond to unsolicited communications and establish communications with another computer.

The problem is that programs can be running and listening for inbound communications without it being obvious. So you want to identify all of the active ports that your computer and verify that they are legitimate.

To determine which ports are open you can use a tool like TCPView from Microsoft (technet.microsoft.com/en-us/sysinternals/bb897437.aspx). Note that the Auditor's office does not make any guarantees regarding the use of reliability of this software.

In the illustration above (note that the window has been resized in order to best show it's contents), the "httpd.exe" program is noted as "listening" on port "80" (marked by the

first red arrow). This means that this computer is running a web server that is ready to provide services. If this is not what you expect to find, disable and/or uninstall the web server software.

In the middle of the above illustration you will see several instances of the "OUTLOOK.EXE" program. Outlook is an example if a program that uses several ports to accomplish its tasks. Notice that OUTLOOK.EXE is listed as being connected to "Remote Address" "172.23.7.12", which is another computer that the OUTLOOK.EXE program is currently connected to and communicating with.

Further down in the above illustration the "iexplorer.exe" program is shown. Because it does not list any "Remote Address" connections, this is simply your web browser running, but not currently retrieving pages.

Near the bottom the "sqlbrowser.exe" program is listed but without a "State" shown. This should be investigated to verify that this is an authorized program.

The last item in the illustration above is the "mysqld.exe" program which is in a "Listening" state, meaning it is ready to provide services to remote computers. This is the mysql database program. Unless you expect your computer to provide database services to other computers, this should be investigated.

To investigate any of these entries, search the internet for the program's full name. This should give you enough information to determine if a given program is of any concern. Note that some websites offer "scanning" programs or services. You do not need to install or run any program from any website in-order to identify a given program. You simply want to checked these lists to see what information they have about the program in question. Below are examples of websites with useful information.

www.processlibrary.com and www.fileresearchcenter.com

Out-dated software

Regularly check all of your software to make sure it is kept up-to-date. This includes the Windows operating system and any applications you have installed. Check the documentation for each program for details about the update process. In most cases software can be configured to automatically update itself as needed. If this option is available, enable it.

Vulnerabilities

Even the most recent version of a program can be vulnerable to different types of exploitation. You can check with the National Vulnerability Database (link shown below) to determine if the version of a program you are using has any publicly known vulnerabilities, and if so, how to correct them.

National Vulnerability Database (web.nvd.nist.gov/view/vuln/search). "NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security check lists, security related software flaws, misconfigurations, product names, and impact metrics. "

Default passwords

Many hardware devices and software programs create default administrative/user accounts when they are installed. Often a default password is assigned for those accounts, possibly without notifying you.

Be sure to check each hardware device and software program on your computer, and network, for these default settings. In each case, set the password to something adequately strong to prevent an attacker from guessing the password and gaining unauthorized access to your system. Also consider changing the user account name if the product allows it. But be sure to document these changes for your own records.

Attackers commonly scan targeted systems and networks looking for devices and programs that have default user accounts and password. When found, and attacker can login without raising any alarms and reconfigure your system, and in many cases penetrate further into your systems.

There are many lists of default passwords as well as product documentation on the internet that make this a very frequent and easy to perform technique.