BinaryHealthcare.com
Industrial Evangelist

10th Jul 2003

Enter The Non-Technical Hacker

By: Adam Chee W.S

Note: This article is also published at TechTutorials.com

Working in the IT industry, I have come across real security experts and self proclaimed "security experts", who are often nothing more than "script kiddies".

Script kiddies are basically "hacker wannabes" who use programs and/or scripts written by other people (real hackers) without understanding how the programs and/or scripts actually work.

Being a script kiddie requires almost no effort because anyone can easily obtain the latest OS and application exploits from security related web sites or forums. In other words, any bored college student who has a connection to the Internet and ample time to spare is capable of being a real threat to your system. Just imagine the number of enemies you have without ever offending anyone.

However, most System Administrators/Engineers perceive script kiddies as nothing more than annoying, but harmless since they lack the technical knowledge to inflict any real damage. This perception cannot be more wrong because there are so many of them out there on the Internet relentlessly trying to do damage. Given the fact that no system is ‘unhackable’, the possibility of your system being comprised is quite high just by looking at the sheer number script kiddies.

So how can you stop these hacker wannabes? The answer lies in understanding how they are capable of posing a threat at all.

As previously mentioned, Script Kiddies have usually little or no technical knowledge and they rely on programs and/or scripts widely available on the Internet. These programs and/or scripts are written by real hackers based on known exploits. Most known exploits have a patch. If not, you can at least disable the service if you don't need it or look for an alternate solution.

In other words, scripts kiddies are usually only an issue if your system is not patched or well protected to begin with because they will most likely succeed only if the System Administrator is lazy, careless or procrastinates in keeping the system secured.

Continued education is critical in maintaining currency as a System Administrator and this cannot be more true when it comes to security issues. Therefore it is of paramount importance that the System Administrator keeps him/herself up-to-date on the latest security exploits and also maintains good system practices such as:

1) Patches
Patch your system regularly to keep it hardened. Most script kiddies' cracks could have been avoided if the patches were applied in time.

2) Minimize services
Do not run any services that you don't need. This will help keep your system secure and efficient. Remember that the less services you run, the less opportunities for attacks.

In addition, essential preventive measures like having a **Firewall** on both your server and the router to the Internet can help minimize the chances of you being a victim of the script kiddies.

Keeping up with security administration is an extremely time consuming task, especially when your actual job is full-time system or network administrator, but it is a task of utmost importance which one cannot afford not to do.

Security is a journey, not a destination.

Contact

Media and all other Queries: media@binaryhealthcare.com

About BinaryHealthcare.com

BinaryHealthcare.com is a vendor-neutral knowledge management repository pertaining to selected IT topics, Healthcare Informatics and its relevant industries (Biomedical Engineering, Radiology, Health Informatics, Telemedicine etc.) for working Professionals, students and anyone who is interested in this unique profession.

For more information, visit www.binaryhealthcare.com