School of Computing & Mathematical Sciences
UNIVERSITY of GREENWICH

Visit: http://cms1.gre.ac.uk/research/csafe

May 2013 Issue #4

This issue:

CSAFE Short Courses

- Computer Forensic Evidence and the Law (Legal Aspects)
- Computer Forensics for Lawyers
- EnCase Computer Forensics 1 and 2 Certification (EnCE©)
- Introduction to Computer Forensics
- Penetration Testing and Vulnerability Assessment

Anonymous Hacks MIT - Calls for New CyberCrime Laws

The hacking group Anonymous took credit for posting messages to Massachusetts Institute of Technology websites calling for an overhaul of computer crime laws.

Anonymous hackers said they also posted tributes to RSS co-founder Aaron Swartz, 26, an outspoken advocate of open information in a legal battle over digital copyright who was found hanged during the weekend in his New York apartment, The Washington Post reported Monday.

Besides being involved in the technology behind RSS, which alerts users to real-time updates on websites, Swartz also had an early role at Reddit and founded the advocacy group Demand Progress.

He believed the articles on the digital library JSTOR should be more widely available, the Post said. He hacked into the database's systems and downloaded articles using a computer hidden in a closet at MIT. When found, Swartz was charged with felony hacking charges and his trial was to begin this spring

In the messages Sunday, Anonymous called for an overhaul of intellectual property and computer crime laws and said Swartz' death should wake up Internet freedom advocates. "We call for this tragedy to be a basis for a renewed and unwavering commitment to a free and unfettered Internet, spared from censorship with equality of access and franchise for all," the group said.

Hispanic Business 14th January 2013

http://www.hispanicbusiness.com/2013/1/14/anonymous_hacks_mit_calls_for_new.htm

Chinese Mobile Users warned about large BotNet Threat

More than 7,000 apps were infected with a trojan, one security firm said. Security researchers say they have discovered a huge botnet running on the smartphones of more than a million unsuspecting mobile users in China.

The devices had been infected by a Trojan-based attack first discovered in 2011, news agency Xinhua reported. The botnet can allow the smartphones to be hijacked remotely and potentially used for fraudulent purposes. The warning comes as mobile internet use in the country has soared, growing by more than 18% in the past year. There are now more than 420 million mobile users, according to the China Internet Network Information Center (Cinic). The surge has attracted the attention of Apple chief executive Tim Cook, who met with the chairman of China Mobile last week. Details of the meeting were scant, but a China Mobile spokesman said it was regarding "matters of co-operation" in the region. While Apple already has deals with two Chinese mobile operators - China Unicom and China Telecom - it is yet to strike a partnership with China Mobile, the biggest operator in the world in terms of subscriber volume.

Security weaknesses

But this latest Trojan warning inflames worries over unlicensed third-party app stores - and the poor awareness among users over possible threats.Unlike Apple's closed system for apps, in which the company must approve all products in its store, Google's platform is far more open. In China specifically, local authorities even went as far as to warn operators to clean up security weaknesses in their mobile app stores. Security firm Kingsoft Duba said last year that the Android.Troj.mdk Trojan had been found in more than 7,000 apps downloaded from non-Google-owned stores. Despite warnings at the time, it is believed that the Trojan is still very much active and enabling the growth of the botnet. Users have been advised to monitor their call and data logs for unusual activity.

BBC News 15th January 2013

http://www.bbc.co.uk/news/technology-21026667

SOFTWARE

“SNORT”

Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire.

Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.

With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS

www.snort.org

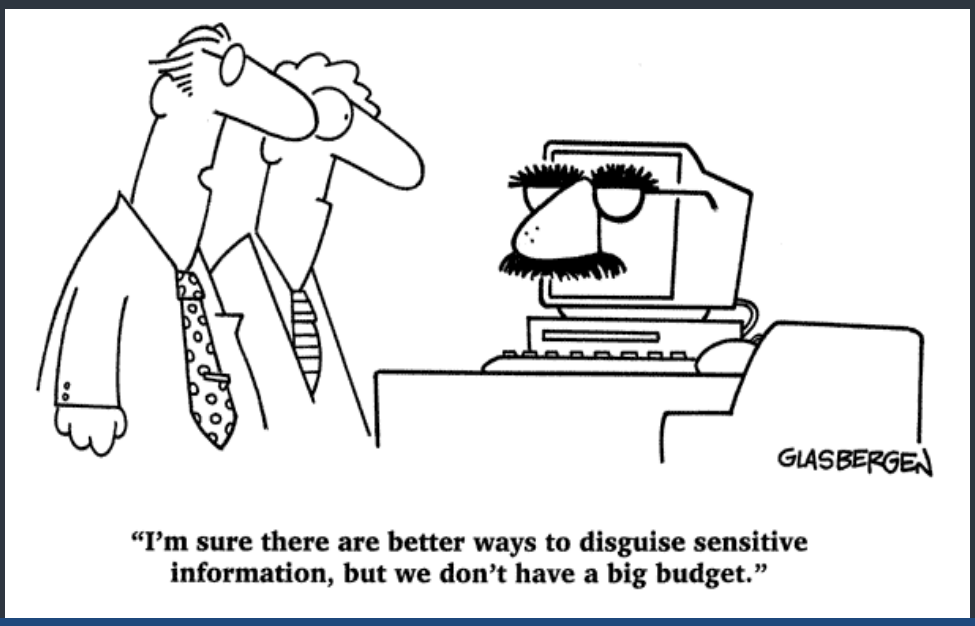
ASK CSAFE A SECURITY QUESTION? ... EXCUSE THE PUN!

With each new issue the CSAFE magazine is introducing new sections to involve readers on a more engaging level.

This section will be for readers to ask CSAFE questions they may have about IT Security. The best questions will be answered extensively and may even have an article based on them!

Please send all questions via CSAFE member email addresses found here:

http://cms1.gre.ac.uk/research/csafe



“I’m sure there are better ways to disguise sensitive information, but we don’t have a big budget.”

About the Author

This month's author:

Yadanar

Yadanar is an MSc student at the University of Greenwich, specialising in the Network & Computer Systems Security. She has been awarded BSc (Hons) equivalent professional certifications by the British Computer Society (BCS). Since then she has been an active member of the organisation.

Yadanar has a very good knowledge in the information security field in both business and technical application.

Contact on:
yadanarhtike@hotmail.co.uk

Penetration Testing - Good or Bad for Business?

By Yadanar, CSAFE Contributing Writer

What is Penetration Testing?

Penetration testing, also known as ethical hacking, enhances the organisational Information Security from numerous perspectives.

In fact, it can never be ensured the degree of reliability of an Information System's security controls, unless the system has actually been broken into and one or more results are analysed. In other words, penetration testing is stepping into the shoes of the *real hackers*, and trying to crack into the organization's current security measures, or identifying if there is any.

Who are the Testers?

Of course, unlike the *real hackers*, whom the business is protecting from, the Penetration Testers or Ethical Hackers are the professional personnel who can test on the system *only* with the organisational consent.

And the competitive Pen-Testers are professionally reliable for their own actions towards the business entities; for instance, ensuring not to test upon the systems and features, other than the ones that are permitted by the organisation.

Why is it Essential?

The Penetration testing is important, because the security of the information itself is crucial for almost all organisations that we can imagine these days.

As a matter of fact, an organisation would like to protect their information for the numerous reasons. Some of those are: to meet the legal obligations, to protect the business reputation, to enhance the Business to Business liaison, etc.

And in order to meet these objectives, Penetration Testing is one of the vital security measures that the business must address upon.

"Penetration testing of IT systems is one of the critical tools through which we provide assurance that our information security regime is appropriately robust and that the data we hold on behalf of the public is secure" Laurie Carter, Information Governance Lead of the Bromley Council

What is the Role of the Information Governance for the Penetration Testing?

The term "Information Governance" has been popularly used, which addresses the enterprise-wide holistic approach to the Information Security that is usually initiated by the strategic-level management of an organization.

And, the Information Governance (IG) policy must enforce the appropriate security measures put in place; which certainly include the practical penetration testing on the organisational systems, in order to analysis the current security level that will be derived from the tests' results and enhance the security further as necessary.

Laurie Carter, the London Borough of Bromley Council's Information Governance Lead agreed with the topic and said "As a Local Authority we have a moral and legal responsibility to protect the information that we use to deliver services to the public, especially where the information is of a personal or sensitive personal nature. Penetration testing of IT systems is one of the critical tools through which we provide assurance that our information security regime is appropriately robust and that the data we hold on behalf of the public is secure".

It's clear that Pen-Testing is essential to running a sound business to address the security goals; and in fact, it is one of the big factors that would give the business a competitive advantage in this information world.