



In this issue:

- 1) Welcome from Peter Wood and Didi Barnes
- 2) Infosecurity Europe, Olympia 25-27 April - *get your free tickets here*
- 3) Peter Wood Speaking at Infosecurity 2005 on 27 April 12:15 – 12:45
- 4) FBTechies in the news
- 5) First Base Technologies – going from strength-to-strength
- 6) White-hats.co.uk
- 7) Check out those probe requests
- 8) Subscription Information

1. Welcome

We are proud to be one of the UK's leading independent security consultancies. We provide penetration testing, web application security testing, network security audits and related security consultancy services. Visit us at www.fbtchies.co.uk.

We hope that the information in this newsletter will be useful to you and would love to get your feedback regarding the content. What would you like to see in future issues? Do you have anything you would like to submit for inclusion? Please feel free to send an email to: webmaven@firstbase.co.uk with your comments.

Peter Wood - Partner (Chief of Operations)
Didi Barnes - Partner (Head of R&D)

2. Infosecurity Europe, Olympia 25-27 April – Get Your Free Tickets

There are now only a few weeks to go until Infosecurity Europe 2006 opens its doors to over 10,000 buyers and sellers in IT Security. Do drop by and visit us at our stand number 242 - we'd love to see you there.

Save £20 by registering FREE today!

Visitors not registered by 21 April will be charged a £20 entrance fee so go to <http://www.fbtchies.co.uk/Content/NewsEvents/Infosec2005/Infosec2005.shtml> to book now...

3. Peter Wood Speaking at Infosecurity 2006

Peter Wood has, for the second year running, been invited to present one of the technical seminars at Infosecurity Europe this year.

The session is entitled "Preventing The Top Five Insider Attacks" and will take place on the Thursday 27 April at 12:15 until 12:45 and Pete will be available for questions afterwards or on our stand.

This seminar (along with the others) is free to attend for visitors so why not come along?

Details of this and the other seminars are on <http://www.infosec.co.uk/page.cfm/Action=Seminars/CategoryID=3/goSection=17>

4. FBTechies in the News

Computer Weekly approached our Chief of Operations, Peter Wood, for the low down on social engineering. The full text of the article appears via the link below:



<http://www.computerweekly.co.uk/Articles/2006/04/04/215129/Firmswarnedtheyarefailingtoblocksocialengineeringattacks.htm>

5. FBTechies – from strength-to-strength

A lot has been going on at FBTechies over the last few months. Our particular blend of top quality penetration testing and consultancy combined with our excellent account management and client support skills has meant our reputation has increased alongside our client base.

Our highly experienced penetration tester, Keiron Northmore, who has been with us for about five years, has been promoted to "Operations Manager". He is responsible for our team of penetration testers, in particular our new penetration tester, Vishal Garg, who started with us last December.

Check out <http://www.fbtechies.co.uk/Content/WhoWeAre/staff.shtml#Vishal> for Vishal's bio. We also plan to take on an additional tester later this year.

We now have our literature in pdf format available direct from our web site www.fbtechies.co.uk.

6. white-hats.co.uk

white-hats.co.uk is our vendor-neutral user group that we set up in May 2002 with the intention of providing a knowledge base and a friendly support group for IT security management and staff. All prospective members undergo a full vetting process, and are expected to sign a confidentiality agreement, prior to being admitted for membership, allowing open discussion of key issues in a confidential environment. Membership comprises, and is open to (provided that they clear vetting), IT security professionals working for UK business and government.

We now have 146 members making this an unique opportunity for networking with your peers via our on-line (members-only) discussion list and our quarterly meetings. Click over to <http://www.white-hats.co.uk/joining.shtml> if you haven't yet joined...

The next meeting is in London on Friday 12 May. Why not come along? Check out www.white-hats.co.uk for more information.

7. Check out those Probe Requests

Do your users have laptops with wireless capability? Are they using them on insecure home wireless networks or public hotspots?

Our Head of R&D, Didi Barnes, comments that as well as checking for any rogue devices, you should analyse the probe request frames issued by client cards using packet capturing techniques. Probe request frames contain the SSIDs of networks that the cards have been used to connect to, even those that are not currently in range.

If you see a probe request containing an SSID of "eurospot" (for example) against a particular wireless card's MAC address, this indicates that the device, e.g. laptop or PDA, containing the wireless card has been used - or gets used - at a public hotspot at some stage. Are your users permitted to use public hotspots? If not, checking probe requests may enable you to monitor - and then discipline - against such activity. If the users are permitted to use public hotspots, anything they send to the access point/s of the hotspot will be unencrypted for anyone to capture unless, for example, PGP encryption is being used where they are using e-mail. The laptop itself could also be



compromised - if the access controls are weak, an attacker could use the wireless hotspot to attempt to connect directly to the laptop...

If you see a probe request containing an SSID of "belkin54g" (for example), this is a default SSID of a commonly used home network access point and may indicate the user is using their laptop or PDA on a home wireless network. A default SSID tends to indicate that if the user hasn't changed the SSID from the default, perhaps there is no encryption and other security in place either. If an attacker were to scan your site, and find an SSID such as this, they could set up an access point to attempt to get the user's card to connect to their evil access point...

So don't just think in terms of preventing rogue access points from being set up in your organisation - keep an eye on what the client devices are - or have been - doing as well!

We will be holding a two-day wireless testing course under our white-hats.co.uk banner which will cover issues such as these in around August-time. If you would be interested in this, please e-mail andy@firstbase.co.uk so we can get an idea of numbers in advance.

8. Subscription Information

We hope that you have found this newsletter to be informative and useful.

This newsletter is intended to be published six times a year. Subscription is free. Please feel free to pass this copy on to friends and colleagues. If you do not wish to receive further copies, please reply to this email with a subject line containing UNSUBSCRIBE NEWSLETTER.

If your friends or colleagues wish to receive the newsletter directly, they should send a request to: webmaven@firstbase.co.uk.

Copyright First Base Technologies 2006

Contact info@firstbase.co.uk or +44 (0)1273 454525 for general information

Web site: www.fbtechies.co.uk

First Base Technologies, Town Hall Chambers, High Street, Shoreham-by-Sea, W Sussex, BN435DD