



## In this issue:

- 1) Welcome from Peter Wood
- 2) Penetration testing: “buy one - get one free”
- 3) Defeating web hackers with WebInspect
- 4) White-hats.co.uk: The new UK ethical hacking group takes off
- 5) Network discovery: finding the holes in your perimeter
- 6) War driving and wireless security
- 7) Testing firewall rulesets: much more than penetration testing
- 8) War dialling and remote access testing
- 9) Subscription Information

## 1. WELCOME

Welcome to the first issue of the First Base Technologies Newsletter.

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.fbtechies.co.uk](http://www.fbtechies.co.uk) >

In the past few months we have established several new partnerships which have broadened our service offerings. Several of these are mentioned below, including Digilog (wireless network audits), SPI Dynamics (WebInspect - web testing software) and Blade Software (Firewall Informer – firewall testing software).

Our counter-hacking group, white-hats.co.uk, is going from strength to strength. Read on for more details or visit < [www.white-hats.co.uk](http://www.white-hats.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 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: [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk) with your comments.

Peter Wood  
Chief of Operations

## 2. PENETRATION TESTING: “BUY ONE - GET ONE FREE”

External penetration tests are designed to provide security assurance for firewalls, routers, mail servers and web servers.

Our tests include whois enquiries for contact details and IP ranges; traceroute to identify intermediate devices; zone transfers to find other hosts in your domain; ping sweeps and port scans to find hosts and services; banner grabbing to identify operating systems and servers;



SNMP queries; and detailed automated scans using ISS Internet Scanner. We test over 1,200 published security vulnerabilities, using both automated and manual exploits.

For November and December, we are offering a full re-test of your Internet connection at no additional charge. This provides a thorough test of your corrective actions following our initial report and gives you that essential double-check entirely free.

Simply place an order for any of our range of external penetration tests during November or December and we will provide a free of charge re-test at a date to suit you. E-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk) for more details or a quotation.

### **3. DEFEATING WEB HACKERS WITH WEBINSPECT**

From the hacker's perspective, access to web applications is virtually unrestricted – firewalls are specifically configured to allow such traffic and are incapable of distinguishing hackers from legitimate users.

A key tool to respond to this threat is automated web application vulnerability testing. This focuses on prevention: examining web content from a hacker's perspective. WebInspect is designed to crawl through entire web sites in order to build a profile of the content and investigate every conceivable avenue that a hacker might follow. The results of the web crawl and investigation are delivered in a comprehensive report that describes every detected vulnerability and suggested fixes.

Automated web-application vulnerability testing is particularly appropriate for applications that facilitate high-value transactions or access to sensitive information. Breaching these applications can jeopardise the organisation's financial performance, intellectual property assets, or brand reputation. The time required for automated testing and fixes is a minor investment with major returns. Moreover, the use of vulnerability testing solutions lets the organisation shift from a reactive to pro-active footing, without relying on the expense of manual penetration testing.

To find out more, to obtain a free evaluation CD or to arrange a demonstration, e-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk)

### **4. WHITE-HATS.CO.UK: THE NEW UK ETHICAL HACKING GROUP TAKES OFF**

White-hats.co.uk - The Intelligent Response to Hackers and Insiders! Formed to help everyone involved in protecting their networks from hackers and insider attacks. There is so much to read, study and respond to ... white-hats.co.uk is a new way of exchanging information and learning about threats as they emerge.



Open only to UK security and IT professionals, white-hats.co.uk is already attracting a large number of members from commercial organisations, government and the security industry < [www.white-hats.co.uk](http://www.white-hats.co.uk) >

The next white-hats.co.uk meeting (Friday 22 November at the Institute of Directors) focuses on “War driving, war chalking and securing your wireless networks”. Simon Gunning of Digilog < [www.digilog.org](http://www.digilog.org) > will present his perspective on this hot topic (see War Driving and Wireless Security below for more on this issue)

The February white-hats.co.uk meeting is entitled “Can your firewall rules take the heat?” and will address the critical area of testing firewall policies in a live environment.

To apply for (free) membership of white-hats.co.uk, e-mail [ailise@firstbase.co.uk](mailto:ailise@firstbase.co.uk)

### **5. NETWORK DISCOVERY: FINDING THE HOLES IN YOUR PERIMETER**

Who can access your corporate data? Most large organisations do not have an accurate, up-to-date picture of their network. Our network discovery service will discover the structure and map the perimeter of your corporate network, highlighting any third-party connections. Using SNMP, ICMP and NetBIOS in a unique blend, we can provide a clear picture of who connects to your network and how you may be vulnerable.

We review router and switch configurations, passwords and SNMP community strings. We investigate third-party connections, dial-in and dial-out facilities, firewalls and edge routers, and set the stage for subsequent penetration tests and vulnerability scans.

E-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk) for more details or a quotation.

### **6. WAR DRIVING AND WIRELESS SECURITY**

In March this year, the BBC reported that “almost all the wireless networks in London are vulnerable to attack”. A comprehensive seven-month audit by Digilog found that 92% of the 5,000 wireless networks in the capital had not taken basic steps to protect themselves against casual attacks. Many of the networks readily handed out internet connections to anyone that connected to them and almost all passed around confidential information in an easy to interpret form.

Even the few that had turned on the basic encryption system were using default settings, making it easy for an attacker to guess the key needed to unscramble data. As a result, anyone gathering up packets of data from these networks would be able to read the text within them easily, according to Simon Gunning of Digilog. Now, war-driving, as it has become known, is a popular pastime with many curious computer enthusiasts.



First Base Technologies, in partnership with Digilog, can conduct a professional wireless audit for your premises, providing you with a comprehensive action plan to secure your wireless networks.

E-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk) for more details or a quotation.

### **7. TESTING FIREWALL RULESETS: MUCH MORE THAN PENETRATION TESTING**

Penetration testing checks your defence against Internet-based hack attacks, but it doesn't check your firewall rules, or whether your firewall is doing that you think it is.

Change management is one of the most difficult tasks facing the firewall administrator. How does the new rule affect the rest of the security policy? Does the latest update to the firewall software break the security policy? Each time something is changed, it has to be thoroughly tested to ensure it does not inadvertently introduce a security risk. Tools like Firewall Informer make it easy for the security professional to validate the condition of a firewall quickly and easily.

Firewall Informer statefully and bi-directionally tests the configuration of a firewall to prove the traffic and protocols that are allowed and blocked by a firewall in both directions. It can test network protocol traffic from any source IP address to any destination IP address using any port.

Conventional port scan technology only gives a very limited view of the firewall policy from the outside in. Manual examination of a firewall policy is a time consuming and difficult exercise and can be prone to human and software errors. Firewall Informer enables us to map your firewall policy outside-in and inside-out and therefore guaranteeing a 100% accurate picture of the security posture of the firewall.

To find out more or to arrange a demonstration, e-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk)

### **8. WAR DIALLING AND REMOTE ACCESS TESTING**

The saying "a chain is only as strong as its weakest link" definitely applies to an unsecured modem on a corporate PC. Companies can spend thousands of pounds on proxies, firewalls, and other solutions aimed at protecting their network. Frequently, however, they overlook the modems attached to PCs all over their the network.

Firewalls can lead to a false sense of protection against external attacks. It's a fact, supported by successful hacker attacks, that firewalls are most easily circumvented by taking a back door - a poorly secured dial-up server or an inadequately policed desktop modem. The unsecured modem provides a weak and often overlooked avenue into some of the most secure networks.



The practice of finding these unsecured modems is referred to as War Dialling. Using professional telephone line scanning software, we call a predefined range of phone numbers and attempt to establish a connection. We identify whether the modem picking up is a fax machine, a data line, or both. The software does the job in three simple steps: connecting to a phone number, identifying the computer system to which the modem at the other end is attached, and attempting to log into that system by automatically trying common user name and password pairs.

E-mail [peter.wood@firstbase.co.uk](mailto:peter.wood@firstbase.co.uk) for more details or a quotation.

### 9. SUBSCRIPTION INFORMATION

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

This newsletter will 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.

If your friends or colleagues wish to receive the newsletter directly, they should send a request to: [info@firstbase.co.uk](mailto:info@firstbase.co.uk)

Copyright First Base Technologies 2002

Contact [info@firstbase.co.uk](mailto:info@firstbase.co.uk) for information

Telephone: +44 (0)1273 454525

Web site: [www.fbtechies.co.uk](http://www.fbtechies.co.uk)

First Base Technologies  
Town Hall Chambers  
High Street  
Shoreham  
West Sussex  
BN43 5DD  
UK