

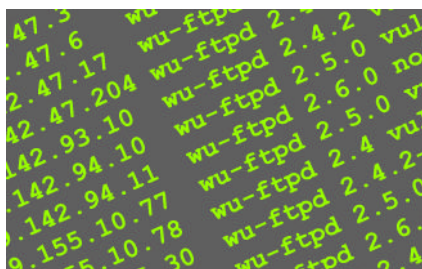
Welcome to the autumn edition of our newsletter — what we're doing and what we see happening.

Giving the Game Away

Is your Internet gateway giving away too many clues to potential intruders?

We were recently asked to investigate a server that had been compromised and was actively being used by a baddie. Our main concern was to block the back door that had been created, clean up the mess and fix the holes that had given unauthorised access in the first place.

An interesting side issue, however, was the use that was being made of this machine. As well as running an Internet Relay Chat server, our intruder was surveying large chunks of IP address space looking for further targets. Specifically, this was a search for old DNS and FTP server software known to have vulnerabilities.



All this was being carried out in a totally automated fashion, using tools circulated on the Internet.

The moral of this story is that it really is worth configuring your servers so that they don't give out version information: it won't improve your absolute security but it will significantly reduce your chances of being attacked in the first place.

The first step is to commission a detailed service analysis of your gateway. Talk to us now if you want to know whether you've left the keys in the door. ◀

e-Security

We are pleased to announce that Idsec now offers the *Open e-Security Platform* (OeSP) from the pioneers in the Real-Time Security Awareness market, e-Security Inc.

Overcoming e-Chaos

Now, we're not going to mention any names, but we know of lots of sites that have built a decent enough security infrastructure but don't handle logs, alarms and event reports properly.

In many cases, the output from firewalls, intrusion detection systems, Web servers and other components just doesn't go

anywhere. Typically, there are a number of consoles that get a cursory look from a system administrator every now and again and the log files are kept for *ad hoc* forensic purposes only. Which is another way of saying that most security related events go unnoticed.

In other words, most security management is far from being real-time: in some cases it can be weeks or even months before a break-in is noticed.



Security you can see

To help solve this problem, and provide system administrators with a single, coherent view of network security, e-Security has developed the OeSP platform.

This allows you to build a centralised security event management system, taking input from different vendor systems and giving you a more complete picture on a single console.

Standard agents allow you to include output from:

<i>Firewall</i>	Raptor, Checkpoint, CyberGuard, WatchGuard, Gauntlet/RID, Cisco PIX, Syslog/Private Eye
<i>Intrusion Detection (network-based)</i>	ISS Real Secure, Net Prowler, Cisco Net Ranger, Network Flight Recorder, CyberCop Network, Dragon
<i>Intrusion Detection (host-based)</i>	Intruder Alert Manager, RealSecure, TripWire, CyberCop Monitor
<i>Operating Systems</i>	NT Event Logs, Solaris and HP-UX syslogs, IBM/Vanguard
<i>Anti-Virus</i>	Symantec, McAfee, Trend Micro's Server Protect
<i>Web Servers</i>	Apache, Microsoft IIS via NT event logs
<i>Databases</i>	Oracle, Sybase, Informix
<i>Policy Monitoring</i>	Axent ESM
<i>Vulnerability Assessment</i>	Internet Scanner
<i>Authentication</i>	Radius Dial-Up Authentication



And, if you need to integrate event messages from other systems, OeSP provides a simple workbench that allows you to create your own agents — without needing programming effort.

Furthermore, any devices that output SNMP traps can be used to send alerts direct to the OeSP console.

Get Going With Idsec

We can get you up and running with a working OeSP system in a surprisingly short time. It takes us just 10 days to get a working pilot system running at your site.

Call us today to find out more. ◀

Read Us On-Line

See our Web site at www.idsec.co.uk for all our services and products. ◀

About Us

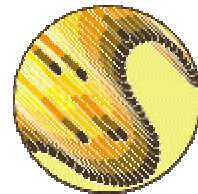
We are independent consultancy specialising in network security.

Idsec can help you examine the security of your enterprise and then advise you on fixing the problems.

Our services cover penetration testing, modem access scans, Internet gateway and network assessment and Internet visibility studies. We also provide training and consultancy for ISS, Sandstorm and e-Security products.



**INTERNET
SECURITY
SYSTEMS**



e-Security™

Idsec
NETWORK SECURITY CONSULTING

Idsec Limited
31-33 College Road
Harrow
Middlesex
HA1 1EJ

Tel: +44 (0) 20 8861 2001
Fax: +44 (0) 20 8861 3433

E-mail: info@idsec.co.uk
WWW: <http://www.idsec.co.uk>