LATERAL | SECURITY

Interesting Vulnerabilities of 2008

Nick von Dadelszen & Ratu Mason
Lateral Security (IT) Services Limited

LATERAL | SECURITY

Company Overview

- Lateral Security (IT) Services Limited
  - Founded in April 2008
  - Head Office - 2 Woodward Street, Wellington
- Company Directors
  - Nick von Dadelszen and Ratu Mason
- Specialist Information Security Services
- “Truly” Independent
  - No vendor alignment
- 7 Security Consultants
  - Management, Technical and Account Management

LATERAL | SECURITY

Talk Objectives

- Give everyone some information on some of the more interesting bugs of 2008
- Explore how previous security decisions fare against future 0day exploits

LATERAL | SECURITY

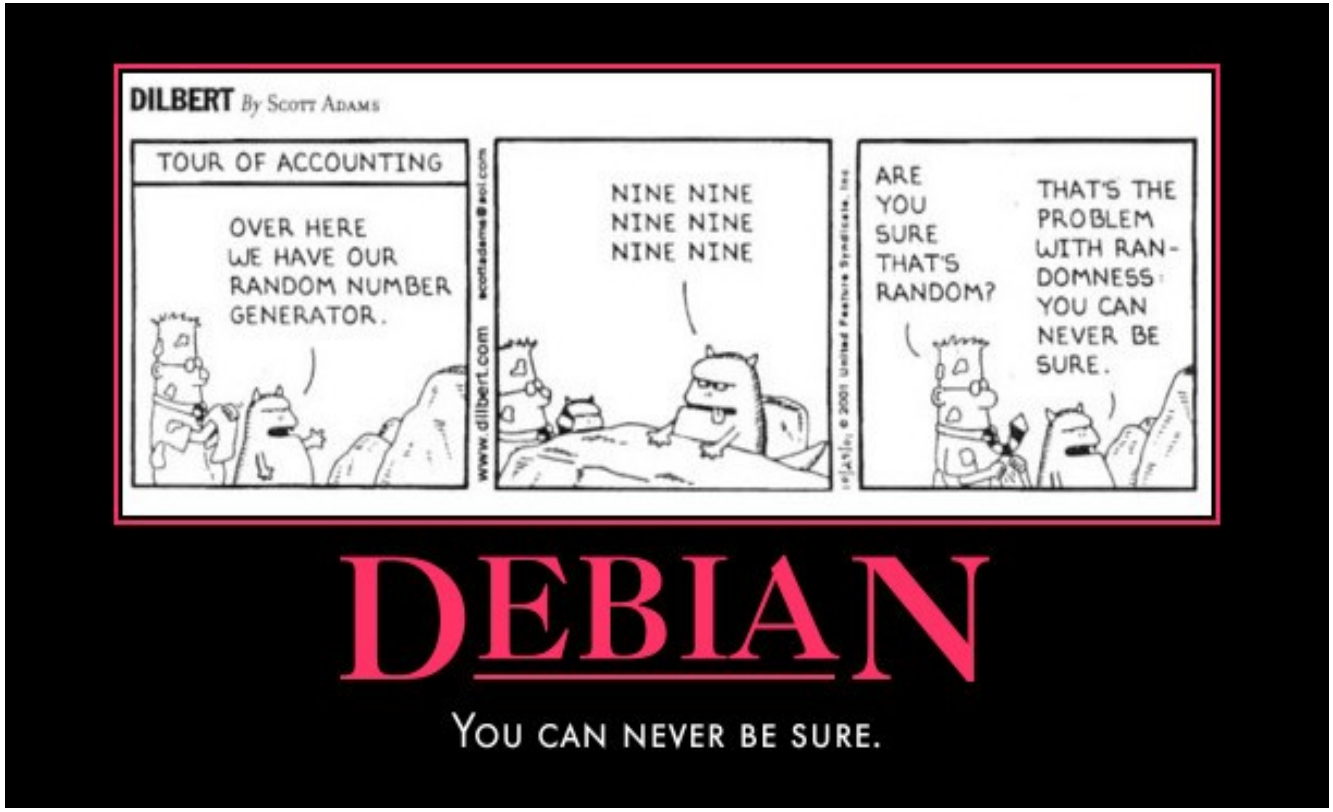
Agenda

- Bugs to discuss:
  - Debian OpenSSL Randomisation
  - SNMP Authentication Bypass
  - Kaminsky's DNS Poisoning
  - Server Service Overflow (MS08-067)
  - SMB Relay Attack (MS08-068)

Debian OpenSSL Randomisation

- CVE-2008-0166 – May 2008
- Debian OpenSSL package removed randomisation during key generation
- Only 32,768 possible keys
- Impacts both SSL and SSH keys generated on a Debian-based system within a 2 year timeframe

Debian OpenSSL Randomisation



LATERAL | SECURITY

Defences

- IP Restrictions
- Least privilege – do not allow root SSH

SNMP Authentication Bypass

- CVE-2008-0960 – June 2008
- SNMP v3 takes authentication hash length from client packet
- Can specify a 1-byte length to reduce potential hashes to 256

Defenses

- Firewalling of SNMP
- Correct security zoning

LATERAL | SECURITY

Kaminsky's DNS Poisoning

- CVE-2008-1447 – July 2008
- Standard TXID forging +
- Random hostname lookups to get around TTL +
- Delegation response to own the whole domain
- Owns vulnerable servers in 10 secs

Defences

- Least privilege – only allow recursive queries from trusted users
- DNSSec (but unrealistic)

Server Service Overflow – MS08-067

- CVE-2008-4250 – October 2008
- Remote code execution in MS Server service
- Found actively being exploited in the wild
- 2000, XP and 2003 authenticated
- Vista and 2008 requires authentication
- Accessible through port 139 and 445

LATERAL | SECURITY

Defences

- Server hardening - Disable unnecessary services
- Firewalling of RPC
- Security zoning

LATERAL | SECURITY

SMB Relay Attack - MS08-068

- CVE-2008-4037 – November 2008
- Ability to reflect SMB NTLM credentials
- Been around for 7 years
- Patch only fixed reflection against the same target, can still reflect against 3rd party

LATERAL | SECURITY

Defences

- Firewalling of SMB
- SMB packet signing
- Security zoning

LATERAL | SECURITY

Summary

- 2008 has been a good year for interesting vulnerabilities
- Patching regularly is still very important however:
- Good security decisions can minimise the impact of future vulnerabilities

LATERAL SECURITY