Copyright © The Last Stage of Delirium Research Group
1996-2004 Poznan, Poland. All rights reserved.

Contact

UNIX Assembly components (shellcodes)

Techniques of writing shellcodes for different operating systems and CPU architectures. Research covers
IRIX/MIPS, HP-UX/PA-RISC, AIX/PowerPC/POWER, Ultrix/ALPHA and Solaris/SPARC platforms
as well as Solaris, Linux, BSD, SCO and BeOS running on Intel x86 processors.

Paper Slides Source Presented at Black Hat 2001 (Las Vegas)

Kernel Level V ulnerabilities (Behind the Scenes of 5th Argus Hacking Challeng   e)

Vulnerabilities and exploitation of OS kernels. Techniques developed and used in a successful attack against
military-grade Argus Pitbull security system and winning 50k USD in the 5th Argus Hacking Challenge.

Paper Slides Source Presented at Black Hat Europe 2001 (Amsterdam) and 18C3 Congress (Berlin)

JAVA and JVM Security V ulnerabilities and their Exploitation T   echniques

Compendium about breaking Java and JVM security. Describes security model (language features, applet
sandbox, security manager, bytecode verifier), classes of vulnerabilities and exploitation methods.

Paper Slides Source Presented at Black Hat Asia 2002 (Singapore)

WIN32 Assembly components (shellcodes)

Project dedicated to research of techniques for writing shellcodes on Windows OS. Presents stealth
and customizable shellcode offering full remote control over compromised machine.

Paper Slides Source Presented at HiverCon 2002 (Dublin)

Micr osoft W indows RPC Security V ulnerabilities

Case study of two very critical remote security issues discovered by the group in 2003 which affected all major
versions of Microsoft Windows and had a huge impact on overall Internet security (Blaster worm).

Slides Source Presented at HITB 2003 (Kuala Lumpur) and Microsoft HQ (Redmond)

Security Myths

[Slides](#) Presented at HITB 2003 (Kuala Lumpur)

Vulnerabilities / Exploits Ar   chive

Proof of concept codes for security vulnerabilities in various operating systems and platforms.
Historical archive - all issues are known, fixed and at this point of time mostly obsolete.

[Irix](#) [Solaris](#) [AIX](#) [HP-UX](#) [SCO](#) [BSD](#) [Linux](#) [Windows](#) [JVM](#)