



Nmap Security Scanner

- [Intro](#)
- [Ref Guide](#)
- [Install Guide](#)
- [Download](#)
- [Changelog](#)
- [Book](#)
- [Docs](#)

Security Lists

- [Nmap Announce](#)
- [Nmap Dev](#)
- [Bugtraq](#)
- [Full Disclosure](#)
- [Pen Test](#)
- [Basics](#)
- [More](#)

Security Tools

- [Password audit](#)
- [Sniffers](#)
- [Vuln scanners](#)
- [Web scanners](#)
- [Wireless](#)
- [Exploitation](#)
- [Packet crafters](#)
- [More](#)

Site News

Advertising

About/Contact

Site Search

Sponsors:



[Full Disclosure](#) mailing list archives

◀ [By Date](#) ▶

◀ [By Thread](#) ▶

Search

[BL4CK] - BL4CK FR1D4Y 2006-07-21

From: redsand <redsand () blacksecurity org>

Date: Fri, 21 Jul 2006 17:13:43 -0500

Welcome to the zer0-day haulocaust.

Exploits - Take a step inside our oven.

Welcome to the zer0-day haulocaust.

Exploits - Take a step inside our oven.

Welcome to the zer0-day haulocaust.

Welcome to the zer0-day haulocaust.

...

(0mg, doesn't this silly poem sound familiar?)

Welcome to the first bl4ck fr1d4y. We have deemed this Friday our first bl4ck fr1d4y of the year. Attached are several fully functional proof of concepts that for the most part, have not hit the security community, as well as fresh code for your eyes.

This is our present to this year's Blackhat/Defcon 2006.

This Fr1d4y's releases:

--[Windows DHCP Client Broadcast Attack
Functioning Remote Exploit for MS06-036
by redsand

--[MDAC Code Execution in Internet Explorer
Functioning Internet Explorer Exploit for MS06-014
by redsand

--[Sendmail 8.13.5 and below Remote Signal Handling exploit
Proof of Concept for the remote signal handling vulnerability

by redsand

```
--[ Solaris SPARC TCP Connect-Back Shellcode (with XNOR Encoded Session)
and Client
SPARC Assembly Shellcode - Connect-Back Shell with an encoded tcp
session
```

by xort

```
--[ Cyrus Imapd - POP3D Exploit
Functioning cyrus-imapd pop3d exploit that will bypass VA Randomization.
Target host gentoo linux 2.6.16
by bannedit
```

Until next time, k33p 1t r34l

This archive can be found at:

http://www.blacksecurity.org/download/61/BL4CK_FR1D4Y_2006-07-21

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>

 [By Date](#)   [By Thread](#) 

Current thread:

- **[BL4CK] - BL4CK FR1D4Y 2006-07-21** *redsand (Jul 21)*
 - [Re: \[BL4CK\] - BL4CK FR1D4Y 2006-07-21](#) *Valdis . Kletnieks (Jul 21)*
 - [RE: \[BL4CK\] - BL4CK FR1D4Y 2006-07-21](#) *dan (Jul 21)*
 - <Possible follow-ups>
 - [\[BL4CK\] - BL4CK FR1D4Y 2006-07-21](#) *redsand (Jul 21)*
 - [RE: \[BL4CK\] - BL4CK FR1D4Y 2006-07-21](#) *John Doe (Jul 22)*

[[Nmap](#) | [Sec Tools](#) | [Mailing Lists](#) | [Site News](#) | [About/Contact](#) | [Advertising](#) | [Privacy](#)]