



STMIK AMIK BANDUNG, 7 MARET 2009

Local Hacking & Pengamanannya

■ ^rumput_kering^

Contents

1

Microsoft Windows RPC Vuln MS08-067

2

Affected Software

3

H D Moore's Metasploit Modul

4

Pengamanan

Apa Itu Hacking?

- ❖ **Programmer sering menggunakan kata-kata hacking dan hacker untuk mengekspresikan kekaguman bagi seseorang yang terampil ahli dalam mengembangkan perangkat lunak**
- ❖ **Hacker berbeda dengan Cracker**
- ❖ **Hacker membangun sesuatu, Cracker merusaknya.**

Microsoft Windows RPC Vuln MS08-067

- ❖ **Menyerang Remote Procedure Call (RPC)**
- ❖ **Ditemukan pada 22 Oktober 2008**
- ❖ **Digunakan pada virus Gimmiv.A**
- ❖ **Critical Vuln. Penyerang bisa menguasai shell/CMD Prompt komputer target**

Affected Software

- » Microsoft Windows 2000 Service Pack 4
- » Windows XP Service Pack 2
- » Windows XP Service Pack 3
- » Windows Server 2003 Service Pack 1
- » Windows Server 2003 Service Pack 2
- » Windows Server 2003 with SP1 for Itanium-based Systems
- » Windows Server 2003 with SP2 for Itanium-based Systems
- » Windows Vista and Windows Vista Service Pack 1
- » Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1
- » Windows Server 2008 for 32-bit Systems*
- » Windows Server 2008 for x64-based Systems*
- » Windows Server 2008 for Itanium-based Systems*

H D Moore's Metasploit Module

❖ http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/smb/ms08_067_netapi.rb

❖ **Berjalan pada:**

- Windows XP SP 1,2,3
- Windows Server 2003
- Windows Vista dan Windows Server 2008 dengan catatan Bisa melalui 3 pengamanan:
 - Data Execution Prevention (DEP)
 - Address Space Layout Randomization (ASLR)
 - Default Password Protection

Pengamanan

- ❖ **Aktifkan Firewall**
- ❖ **Selalu Update Windows Anda**
- ❖ **Beralih ke Linux :-)**

Referensi:

- ❖ <http://www.metasploit.org/>
- ❖ <http://www.securityfocus.com/>
- ❖ <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>



Thank You !

