

All Attacks

Segment Group: All
Attack Type: Permits+Blocks
Severity: All
From: Thu Dec 21 20:00:45 UTC 2006
To: Thu Dec 28 20:00:45 UTC 2006

No.	Filter Name	Severity	Hits
1	4602: MS-RPC: Microsoft Server Service Buffer Overflow	Critical	277
2	4193: SMB: ASN.1 Bitstring Processing Heap Overflow	Critical	212
3	1473: MS-SQL: Resolution Service Buffer Overflow (General)	Critical	112
4	3677: MS-RPC: Windows PlugnPlay Request Anomaly	Critical	105
5	1456: MS-SQL: Slammer-Sapphire Worm	Critical	103
6	2292: MS-RPC: DCOM IRemoteActivation Overflow	Critical	65
7	2289: MS-RPC: DCOM ISystemActivator Overflow	Critical	61
8	2755: MS-RPC: LSASS Active Directory Interface Overflow	Critical	50
9	2966: Spyware: SaveNow/WhenU Pop-up Advertisements	Low	47
10	3990: Metasploit: Metasploit Shellcode	Major	34
11	3139: Spyware: MyWay/MyWeb/MySearch Search Bar Information Transfer	Low	27
12	2965: Spyware: SaveNow/WhenU Program Download	Low	15
13	4616: MS-RPC: Microsoft Server Service Fragmented Request	Critical	9
14	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port	Critical	8
15	2226: Backdoor: TCP Window Size 55808 Trojan	Minor	3
16	0321: Nmap scanner: FUP OS Fingerprinting Probe	Minor	2
17	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Minor	2
18	4307: HTTP: ASN.1 Bitstring Processing Heap Overflow	Critical	2
19	4110: Spyware: WhenU Program Download	Low	1
20	3863: Spyware: MyWay/MyWeb/MySearch Search Bar Program Download	Low	1
21	0092: Loki: Default Client Communications (Little Endian)	Critical	1
22	0091: Loki: Default Client Communications (Big Endian)	Critical	1
23	0290: Invalid TCP Traffic: Possible Recon Scan (SYN FIN)	Minor	1
24	0317: Nmap scanner: NULL OS Fingerprinting Probe	Minor	1