



Security Update: The view from AS1213

Rob Gallagher - rob.gallagher@heanet.ie



Overview

- SSH attacks
- Handling compromised machines
- Web Applications
- IDS

SSH Bruteforcing

```
Dec 10 21:30:31 tachikoma sshd[2493]: refused connect from 210.123.39.112 (210.123.39.112)
Dec 10 21:41:36 tachikoma sshd[2532]: refused connect from 61.163.231.68 (61.163.231.68)
Dec 10 21:42:17 tachikoma sshd[2533]: refused connect from 210.123.39.112 (210.123.39.112)
Dec 11 13:45:16 tachikoma sshd[6253]: refused connect from 82.175.124.76 (82.175.124.76)
[rob@tachikoma] >> []
```

- SSH attacks: low-hanging fruit
- The usual random usernames pattern
- Denyhosts - blacklist
- New attacks: Distributed scanning
 - <http://isc.sans.org/diary.html?storyid=3529>



Compromised Hosts

- Gaining access is sometimes a problem...
- Logfiles
- Rootkit detection
 - Integrity verifiers, eg: Integrit
- Spam/Botnet controllers
 - ..or phishing sites

Web Applications

- Drupal, Moodle, Wordpress, \$CMSOFTHEWEEK
 - Require regular care and feeding
 - Popular attack vector
- Apache reverse proxy
- mod_security
 - Detect and block standard attacks (XSS, SQL injection) and other protocol anomalies

IDS

SURF IDS INTRUSION DETECTION SYSTEM

Logged In as: admin Tuesday 11 Dec 2007 16:12 Active sensors 1 of 1

Home | Report | Analyze | Configuration | Administration

Home Period: 7 day(s) From: 10-12-2007 00:00 Until: 17-12-2007 00:00

Attacks

Detected connections	Statistics
Possible malicious attack [?]	775 ↘
Malicious attack [?]	48 ↘
Nepenthes	48 ↘
Malware offered [?]	48 ↘
Malware downloaded [?]	11 ↘

Exploits

Malicious attacks	Statistics
DCOM	21 ↘
IIS	20 ↘
ASN1	7 ↘
Total	48 ↘

Attackers

IP Address	Last Seen	Total Hits
80.91.83.19	11-12-2007 02:17:06	363 ↘
201.70.100.124	10-12-2007 17:54:41	181 ↘
193.1.228.130	10-12-2007 17:04:11	53 ↘
83.143.86.194	11-12-2007 14:38:48	40 ↘
88.12.44.50	10-12-2007 21:25:32	22 ↘
89.136.31.252	10-12-2007 20:43:10	22 ↘
58.239.157.69	11-12-2007 04:08:55	22 ↘
81.216.181.183	10-12-2007 20:36:58	22 ↘
190.66.179.248	10-12-2007 17:26:13	20 ↘
24.152.233.84	11-12-2007 07:52:11	13 ↘

Last Seen: █ Today █ █ █ █ 7 days ago

Ports

Destination Ports	Description	Total Hits
445	microsoft-ds	446 ↘
139	netbios-ssn	249 ↘
80	http	31 ↘
135	msrpc	24 ↘
4444	No description	17 ↘
1025	No description	10 ↘
3372	No description	10 ↘
9988	No description	7 ↘
110	pop3	3 ↘
1023	No description	2 ↘

HEAnet version: 2.00 | <http://ids.heanet.ie> HEAnet

- Based on SurfNet IDS
- Distributed IDS
- <http://ids.heanet.ie>