

セキュリティ関連

主にスクリプト kiddy と思われるアタックのログの一部を晒しておく。

2006/02/25

Feb 25 20:20:24 ushi sshd[67052]: Illegal user pinter from 61.31.199.70

Feb 25 20:20:25 ushi sshd[67055]: Address 69.90.123.51 maps to mail.everettandso

lsvig.com, but this does not map back to the address - POSSIBLE BREAKIN ATTEMPT!

2005/12/21

日本人名のアカウントをスキャンしてきたので注意

Dec 21 02:06:57 ushi sshd[33449]: Illegal user iwamotos from 61.111.254.83

Dec 21 02:06:58 ushi sshd[33451]: Illegal user iwamori from 61.111.254.83

2005/12/04

日本人名のアカウントをスキャンしてきたので注意

Dec 4 00:38:00 ushi sshd[76455]: Illegal user kazuki from 211.253.7.15

Dec 4 00:38:01 ushi sshd[76457]: Illegal user kazuya from 211.253.7.15

2005/11/04

Nov 4 14:19:22 ushi sshd[77929]: Illegal user akio from 69.19.225.155

Nov 4 14:19:22 ushi sshd[77929]: reverse mapping checking getaddrinfo for colo-
rev155.sac1.networkoneit.com failed - POSSIBLE BREAKIN ATTEMPT!

Nov 4 14:19:22 ushi sshd[77931]: warning: /etc/hosts.allow, line 28: can't veri
fy hostname: getaddrinfo(colo-rev155.sac1.networkoneit.com, AF_INET) failed

Nov 4 14:19:22 ushi sshd[77931]: refused connect from 69.19.225.155 (69.19.225.155)

2005/10/29

日本人名のアカウントをスキャンしてきたので注意

Oct 29 09:06:43 ushi sshd[15087]: Illegal user takahashi from 211.60.75.199

Oct 29 09:06:44 ushi sshd[15089]: Illegal user tanaka from 211.60.75.199

2005/10/28

日本人名のアカウントをスキャンしてきたので注意

Oct 28 06:55:49 ushi sshd[5414]: Illegal user uketsuke from 61.152.160.155

Oct 28 06:55:51 ushi sshd[5416]: Illegal user shinjin from 61.152.160.155

2005/10/11

かなりしつこかったようだ

Oct 11 07:51:12 ushi sshd[50806]: Illegal user yoshida from 218.234.130.16

Oct 11 07:51:13 ushi sshd[50808]: Illegal user tunekeyo from 218.234.130.16

2005/10/10

日本人名のアカウントをスキャンしてきたので注意

SOct 10 01:00:33 ushi sshd[37289]: Illegal user siranui from 213.193.253.165

Oct 10 01:00:36 ushi sshd[37291]: Illegal user matsumi from 213.193.253.165

2005/09/30

スキャンは外人名のみ

Sep 29 20:11:19 ushi sshd[95905]: Illegal user ashley from 210.212.85.4

Sep 29 20:11:23 ushi sshd[95907]: Illegal user bandit from 210.212.85.4

2005/09/20

スキャンは外人名のみ

Sep 20 05:07:19 ushi sshd[78354]: Illegal user fengyuan from 66.88.64.195

Sep 20 05:07:26 ushi sshd[78358]: Illegal user nisuser from 66.88.64.195

Sep 20 09:42:35 ushi sshd[80098]: Illegal user bela from 81.102.8.152

Sep 20 09:42:37 ushi sshd[80100]: Illegal user pantera from 81.102.8.152

2005/09/19

日本人名のアカウントをスキャンしてきたので注意

Sep 19 00:27:21 ushi sshd[65920]: Illegal user sakai from 202.229.26.205

Sep 19 00:27:22 ushi sshd[65922]: Illegal user shimada from 202.229.26.205

2005/09/16

スキャンは外人名のみ

Sep 16 07:27:22 ushi sshd[40702]: Illegal user nicole from 218.214.19.209

Sep 16 07:27:27 ushi sshd[40704]: Illegal user send from 218.214.19.209

逆引き無し

Sep 16 15:00:04 ushi sshd[43583]: Illegal user abinitioforum from 70.87.122.212

Sep 16 15:00:04 ushi sshd[43583]: reverse mapping checking getaddrinfo for 212.70-87-122.reverse.theplanet.com failed - POSSIBLE BREAKIN ATTEMPT!

Sep 16 15:00:04 ushi sshd[43585]: warning: /etc/hosts.allow, line 28: can't verify hostname: getaddrinfo(212.70-87-122.reverse.theplanet.com, AF_INET) failed

スキャンは外人名のみ

Sep 16 20:35:20 ushi sshd[46785]: Illegal user test2 from 210.106.165.201

Sep 16 20:35:22 ushi sshd[46787]: Illegal user test3 from 210.106.165.201

2005/09/15

日本人名のアカウントをスキャンしてきたので注意

Sep 15 11:12:38 ushi sshd[32797]: Illegal user inosisino from 61.103.229.40

Sep 15 11:12:40 ushi sshd[32799]: Illegal user ishii from 61.103.229.40

Sep 15 11:12:41 ushi sshd[32801]: Illegal user ishikawa from 61.103.229.40

逆引きなし

Sep 15 15:47:13 ushi sshd[34466]: Illegal user djphummer from 200.62.179.67

Sep 15 15:47:13 ushi sshd[34466]: reverse mapping checking getaddrinfo for host-

2005/09/12

日本人名のアカウントをスキャンしてきたので注意

16分ほど攻撃を続けてきた

Sep 12 07:05:55 ushi sshd[90561]: Illegal user tadami from 221.147.5.145

Sep 12 07:05:58 ushi sshd[90563]: Illegal user tadao from 221.147.5.145

Sep 12 07:06:00 ushi sshd[90565]: Illegal user taichi from 221.147.5.145

2005/09/11

スキャンは外人名のみ

Sep 11 16:47:00 ushi sshd[84800]: Illegal user stephane from 130.161.21.93

Sep 11 16:47:02 ushi sshd[84804]: Illegal user theodore from 130.161.21.93

2005/09/10

スキャンは外人名のみ

Sep 10 07:51:49 ushi sshd[72919]: Illegal user nicole from 60.248.148.131

Sep 10 07:51:51 ushi sshd[72921]: Illegal user paul from 60.248.148.131