Analysis of Malicious SSH Login Attempts Observed in Low-Interaction Honeypots

Jim Owens

Advisor: Jeanna Matthews

Overview

- Motivation
- Background
- Methodology
- Observations
- Analysis
- Conclusions
- Future work

Motivation

- Passwords are widely used
- Linux systems are popular targets
  - 43% of spam originates from Linux systems
  - Linux systems highly prized for botnet use
- SSH brute-force attacks are common
  - One DenyHosts file contains ~4,900 banned IPs active* within the past four weeks
  - Another file contains >30,000 IPs active* since mid-February (no purging)

*__active__: 3+ distinct attacks in >5-hour period among ~6,800 servers

Background

- Secure Shell (SSH)
  - Client/server network protocol (TCP port 22)
  - Provides end-to-end encryption of network traffic, using public-key cryptography
  - Supports remote login, file transfer & tunneling of arbitrary TCP traffic
- OpenSSH
  - Open source version developed by OpenBSD
  - As of 2005, most widely used SSH version

Background

- By default, OpenSSH-server
  - Allows unlimited login attempts
  - Logs all attempts, successful or not
  - Does *not* log passwords

```
Oct 15 05:58:01 peru sshd[24906]: Invalid user lpa from 67.16.84.4
Oct 15 05:58:04 peru sshd[24906]: Failed password for invalid user
lpa from 67.16.84.4 port 34292 ssh2
Oct 15 05:58:05 peru sshd[24908]: Invalid user admin from 67.16.84.4
Oct 15 05:58:07 peru sshd[24908]: Failed password for invalid user
admin from 67.16.84.4 port 35258 ssh2
Oct 15 05:58:08 peru sshd[24910]: Invalid user admin from 67.16.84.4
Oct 15 05:58:10 peru sshd[24910]: Failed password for invalid user
admin from 67.16.84.4 port 35604 ssh2
```

Background

- Creating strong passwords*
  - Make it lengthy (8+ characters)
  - Combine letters, numbers, and symbols
  - Use words and phrases that are easy for you to remember, but difficult for others to guess

*_Strong passwords: How to create and use them,_ http://www.microsoft.com/protect/yourself/password/create.mspx

Background

- Strong passwords?

yPWM5LHGAh	P0oByo@b
E5efEHW65	Wesam@200
2borNOT2b	Goethe6750
FD6d95oE	68jjj167@102
I7IVCOivaV	ukJ33W_QoO
JagGolUie-720	5tgb6yhn#P

Methodology

- Experimental setup modeled on a recent NZ Honeynet Alliance project, as reported in 9/2006 *SecurityFocus* article
  - Password collection part of more general high-interaction experiment
  - Included one standard RedHat 9 server
  - Honeywall used to log/control attack traffic
  - SSH server patched to also log passwords
  - SSH brute-force attacks allowed to succeed

Methodology

- Experimental setup
  - Three low-interaction honeypots
    - Ubuntu 6.10 server on campus network (zilch)
    - “Off-duty” Fedora Core 6 teaching server on a Business DSL network (peru)
    - Ubuntu 6.04 server VM on a production desktop system on a residential DSL network (satie)
  - Honeypots' OpenSSH servers patched to log passwords
  - SSH brute-force attacks *not* allowed to succeed

Methodology

```
int auth_password(Authctxt *authctxt, const char *password) {

   struct passwd * pw = authctxt->pw;
   int result, ok = authctxt->valid;

   /* JPO 7/11/07 Added: Log all passwords */
   if( strlen(password) > 0 )
     logit("PW-ATTEMPT: %s from %s", password, get_remote_ipaddr());

   if (*password == '\0' && options.permit_empty_passwd == 0)
      return 0;

   /* JPO 7/11/07 Changed: Disallow all logins */
   /* result = sys_auth_passwd(authctxt, password); */
   result = 0;

   if (authctxt->force_pwchange)
      disable_forwarding();

   return (result && ok);
} /* OpenSSH server on port 22 */
```

Methodology

```
Aug 25 21:38:33 peru sshd[27702]: Invalid user test from 61.146.178.8
Aug 25 21:38:33 peru sshd[27702]: PW-ATTEMPT: test from 61.146.178.8
Aug 25 21:38:41 peru sshd[27704]: Invalid user guest from 61.146.178.8
Aug 25 21:38:41 peru sshd[27704]: PW-ATTEMPT: guest from 61.146.178.8
Aug 25 21:38:45 peru sshd[27706]: Invalid user admin from 61.146.178.8
Aug 25 21:38:45 peru sshd[27706]: PW-ATTEMPT: admins from 61.146.178.8
Aug 25 23:35:01 peru sshd[27905]: Invalid user staff from 202.141.47.83
Aug 25 23:35:01 peru sshd[27905]: PW-ATTEMPT: staff from 202.141.47.83
Aug 25 23:35:04 peru sshd[27907]: Invalid user sales from 202.141.47.83
Aug 25 23:35:04 peru sshd[27907]: PW-ATTEMPT: sales from 202.141.47.83
Aug 25 23:35:07 peru sshd[27909]: Invalid user recruit from 202.141.47.83
Aug 25 23:35:07 peru sshd[27909]: PW-ATTEMPT: recruit from 202.141.47.83
Aug 25 23:35:10 peru sshd[27911]: Invalid user alias from 202.141.47.83
Aug 25 23:35:10 peru sshd[27911]: PW-ATTEMPT: alias from 202.141.47.83
Aug 25 23:35:13 peru sshd[27913]: Invalid user office from 202.141.47.83
Aug 25 23:35:13 peru sshd[27913]: PW-ATTEMPT: office from 202.141.47.83
```

Observations

- **zilch** (dedicated system on campus net)
  - 43 attacks in 36 days; 13,567 login attempts; min: 2, max: 3,679; average: 331
- **peru** (server on business DSL)
  - 55 attacks in 34 days; 9,082 login attempts; min: 1, max: 2,195; average: 172
- **satie** (VM server on residential DSL net)
  - 26 attacks in 40 days; 11,940 login attempts; min: 1, max: 9,311, average: 478

Observations

Source IPs

- **zilch** (43 attacks)
  - 41 distinct IPs; one also attacked satie
- **peru** (55 attacks)
  - 53 distinct IPs; one also attacked satie
- **satie** (26 attacks)
  - 25 distinct Ips
- 113 (96%) of observed source IPs listed in DenyHosts database

Analysis

Attack profiles

- 30 of 124 (24%) attacks used obvious scripts or username/password lists
  - Script-9* (11 attacks, on all honeypots)
  - Script-66 (3 attacks, on 2 honeypots)
  - Script-168 (13 attacks, on all honeypots)
  - Script-363 (3 attacks, on 2 honeypots)

*At least two partial runs also observed

Analysis

Script-9

Username	Password
test	test
guest	guest
admin	admins
admin	admin
user	user
root	password
root	root
root	123456
test	123456

Analysis

Usernames

- **zilch** (13,567 attempts, campus net)
  - 2,835 unique usernames, 71% of actual users
  - root targeted in 40% of attempts
- **peru** (9,082 attempts, business DSL)
  - 2,948 unique usernames, 41% of actual users
  - root targeted in 18% of attempts
- **satie** (11,940 attempts, residential DSL)
  - 2,027 unique usernames, 79% of actual users
  - root targeted in 24% of attempts

Analysis

Passwords

- **zilch** (13,567 attempts, campus net)
  - 5,604 unique passwords
  - 1,449 dictionary* words (26%)
- **peru** (9,082 attempts, business DSL)
  - 4,552 unique passwords
  - 881 dictionary* words (19%)
- **satie** (11,940 attempts, residential DSL)
  - 3,936 unique passwords
  - 544 dictionary* words (14%)

**dictionary: Includes 57,025 American-English words*

Analysis

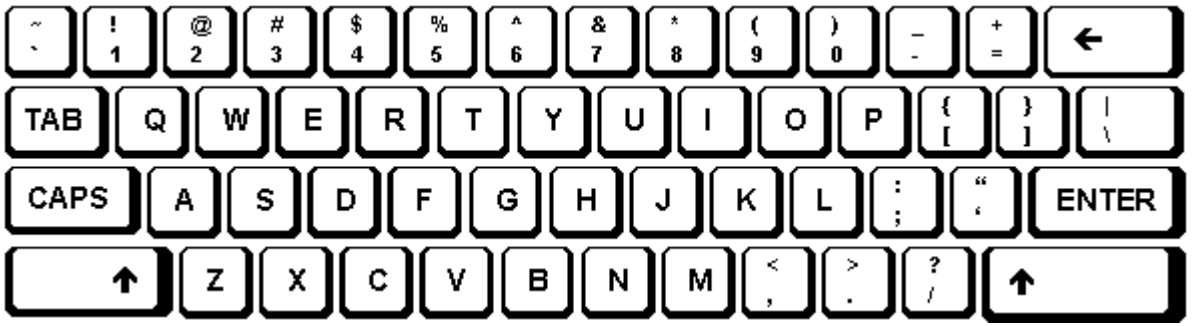
Top 20 passwords

123456	123456	123456
password	password	12345
12345	test	password
test	admin	**123**
1234	root	**1234**
123	admin123	test
admin	**qwerty**	test123
root	passwd	passwd
test123	test123	1
passwd	**mysql**	12
abc123	user	root
guest	administrator	admin
linux	apache	**abc123**
mysql	guest	**qwerty**
webmaster	**master**	1q2w3e
administrator	passwd123	asdfgh
master	webadmin	abcd1234
pass	**webmaster**	user
user	12345	guest
temp	**linux**	administrator

Analysis

Patterns:

1qa2ws3ed	0o9i8u7y
bhunjimkolp	o9q1w2e3i8u7
q2w3e4r5	!@#$%^
2wsx3edc	zdxfcgvh
5tgb6yhn	zsexdrcft
0plmnko9	qpwoeiruty



Analysis

1337 (leet):

un1v3rs3	m1tn1ck
il0v3y0u	@ct10n
ma1ls3rv3r	blu3j3@ns
r3dh@t	m00nl1ght
n0chanc3	l3tm31ns1de
mak3l0ve	h4cks4f3
p@55wd	d1sc0v3ry
m4gn3t	b4ckm3upsc077y

Analysis

- Strong passwords?

yPWM5LHGAh	P0oByo@b
E5efEHW65	Wesam@200
2borNOT2b	Goethe6750
FD6d95oE	68jjj167@102
I7IVCOivaV	ukJ33W_QoO
JagGolUie-720	5tgb6yhn#P

All were collected in the honeypots!

Conclusions

- Brute-force SSH attacks represent a real threat to networked Linux systems
- Many Linux admins and users employ simple username/password combinations, perhaps for temporary accounts
- Attackers share username/password lists
- Attackers target accounts using “strong” passwords based on physical patterns, leets, and other schemes

Future work

- Expand data collection to include network scans prior to attacks
- Attempt to automate the process of pattern identification
- Attempt to recognize passwords based on familiar creation patterns
- Create a Web site where visitors can test passwords against a real-time database of passwords actually used in attacks

Questions & comments