SSH Security Tips

Analysis & Prevention

```
grep 'Failed password' /var/log/auth* | grep sshd | wc -l
```

2458

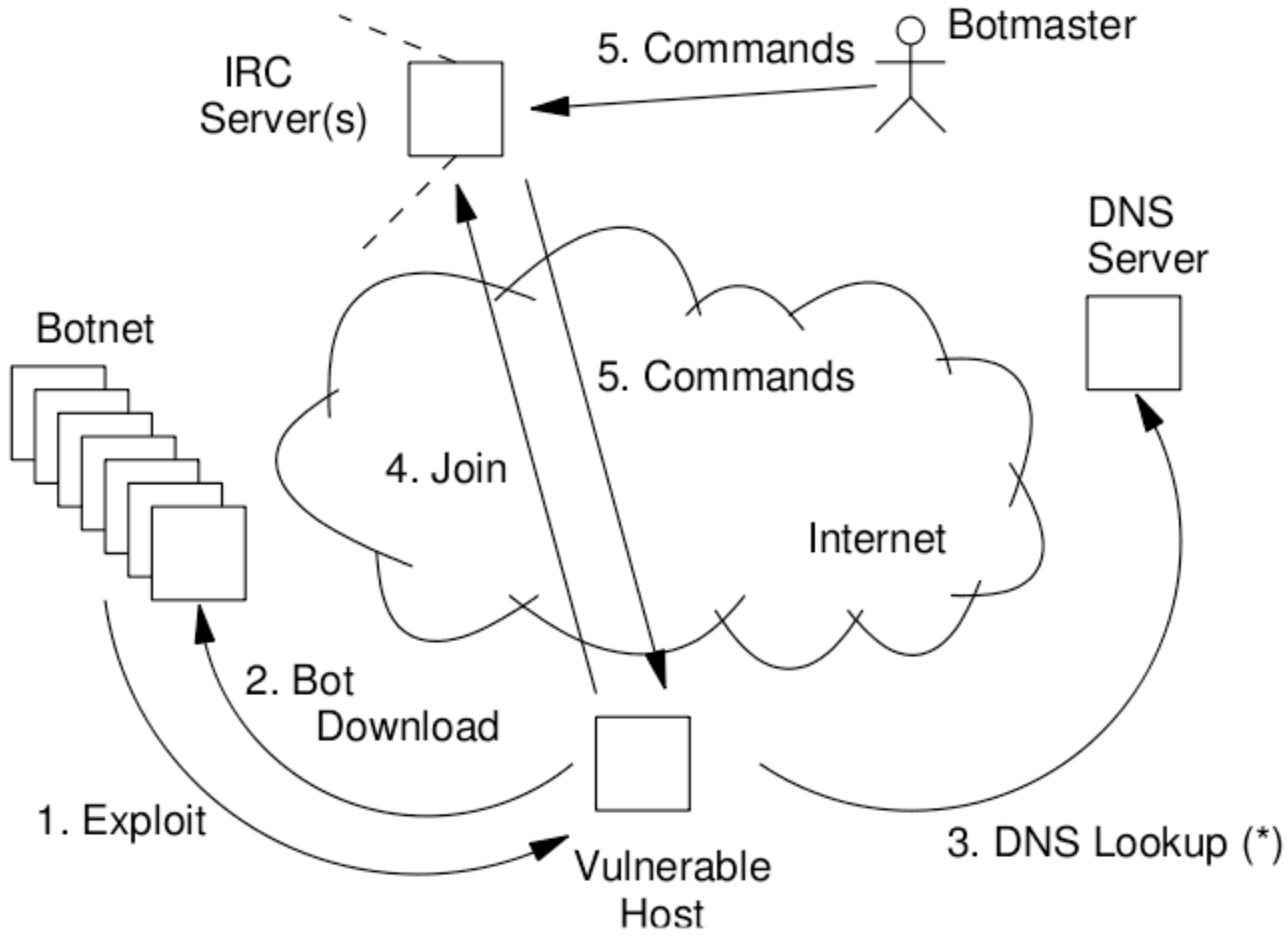
"Is it normal to get hundreds of break-in attempts per day?"

- Some guy on Serverfault

Sadly, yes.

Automated dictionary attacks

Usually part of a botnet


IRC
Server(s)
5. Commands
Botmaster
DNS
Server
Botnet
5. Commands
4. Join
Internet
2. Bot
Download
1. Exploit
Vulnerable
Host
3. DNS Lookup (*)

What can we do?

Use strong passwords/usernames

vi /etc/ssh/sshd_config

Disallow root logins

```
PermitRootLogin no
```

Use public-key authentication
and disable password auth completely.

```
PubkeyAuthentication yes
PasswordAuthentication no
```

ssh-keygen -t rsa

cat id_rsa.pub >> ~/.ssh/authorized_keys

AllowUsers alice bob@150.140.*.*

Denyhosts / Fail2ban / OSSEC

Netfilter rate-limiting

```
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --set

iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --update
--seconds 60 --hitcount 4 -j DROP
```

Port knocking &
Single Packet Authorization

Popular implementations: fwknop, knockd

Cool Sunday afternoon project:

Two-factor SSH authentication with Google Authenticator

VPN

(More likely in a corporate environment)

Honeypots

What is a honeypot?

A security mechanism designed to lure malicious activities – Analyze them

Classes

High: Full functional interaction

Low: limited functionality (emulated services)

Kippo – SSH Honeypot

http://code.google.com/p/kippo/

Medium Interaction (combined characteristics)

Log SSH brute force attacks & shell interaction

Python based

Still under development

FEATURES

Fake shell based on Debian 5

Fake file system – add/remove ability

Fake file contents

Fake command outputs

Saved wget downloaded files

UML compatible logs

KIPPO TOOLS

playlog.py - utility to replay session logs

createfs.py - used to create fs.pickle

passdb.py – add/remove/list passwords

Information about the attacker

Used SSH agent

Used username/passwords

Timings (bot or human)

DEMO TIME

http://serverfault.com/questions/244614/is-it-normal-to-get-hundreds-of-break-in-attempts-per-day

http://www.cyberciti.biz/tips/ssh-public-key-based-authentication-how-to.html

http://www.cipherdyne.org/fwknop/

http://www.zeroflux.org/projects/knock

http://denyhosts.sourceforge.net/

http://www.fail2ban.org/