Understanding VPS Security via SSH

Pat Pannuto / Marcus Darden / Cameron Gagnon (for today!)

Today's Definitions

- VPS

Today's Definitions

- VPS

- PAM

Today's Definitions

- VPS
- PAM
- SPAM

Today's Definitions

- VPS
- PAM
- SSH

Really Today's Definitions

- Virtual Private Servers (VPS)
- Pluggable Authentication Modules (PAM)
- Secure SHell (SSH)

Really Today's Definitions

- Virtual Private Servers (VPS)
  - Homework 1!
- Pluggable Authentication Modules (PAM)
- Secure SHell (SSH)

Really Today's Definitions

- Virtual Private Servers (VPS)
  - Homework 1!
- Pluggable Authentication Modules (PAM)
- Secure SHell (SSH)
  - Matt's post on Piazza!

Now You Know

Project's Goal

- Show us the passwords of people (or programs) trying to authenticate to the Virtual Private Server

Project's Goal

- Show us the passwords of people (or programs) trying to authenticate to the Virtual Private Server

Lecture's Goal

- Show how knowledge from this class can be applied

Setting up a Virtual Private Server

- What do you do when you first set up a new computer, phone, or personal device?

Setting up a Virtual Private Server

- What do you do when you first set up a new computer, phone, or personal device?

Dotfiles

- Homework 12!

Setting up a Virtual Private Server

- What do you do when you first set up a new computer, phone, or personal device?

Dotfiles

- Homework 12!

`~/.ssh/config`

```
Host c4cs-lecture
    Hostname 138.236.11.81
    User root
    IdentityFile ~/.ssh/id_rsa_do_pnu
```

- Regular and Advanced Homework 12

Let's dive in

- https://github.com/cameron-gagnon/ssh_pass_logging

Make and `Makefile`s

- Homework 7!

Installing the PAM module

Where did we learn how programs get configuration information?

Installing the PAM module

Where did we learn how programs get configuration information?

- Lecture 3!

Installing the PAM module

Where did we learn how programs get configuration information?

- Lecture 3!

Alternatives to a PAM module

- Install and compile OpenSSH from source while adding this patch.
- Would get to tie in package managers (Week 12!)

Scripting

```
# from create_initial_users.sh

# list of some default usernames to add
while IFS='' read -r user || [[ -n "$user" ]];
do
    ./honeypot_user.sh "$user"
done < "usernames.txt"
```

- Regular and Advanced Homework 3
- Advanced Homework 6

Piping commands

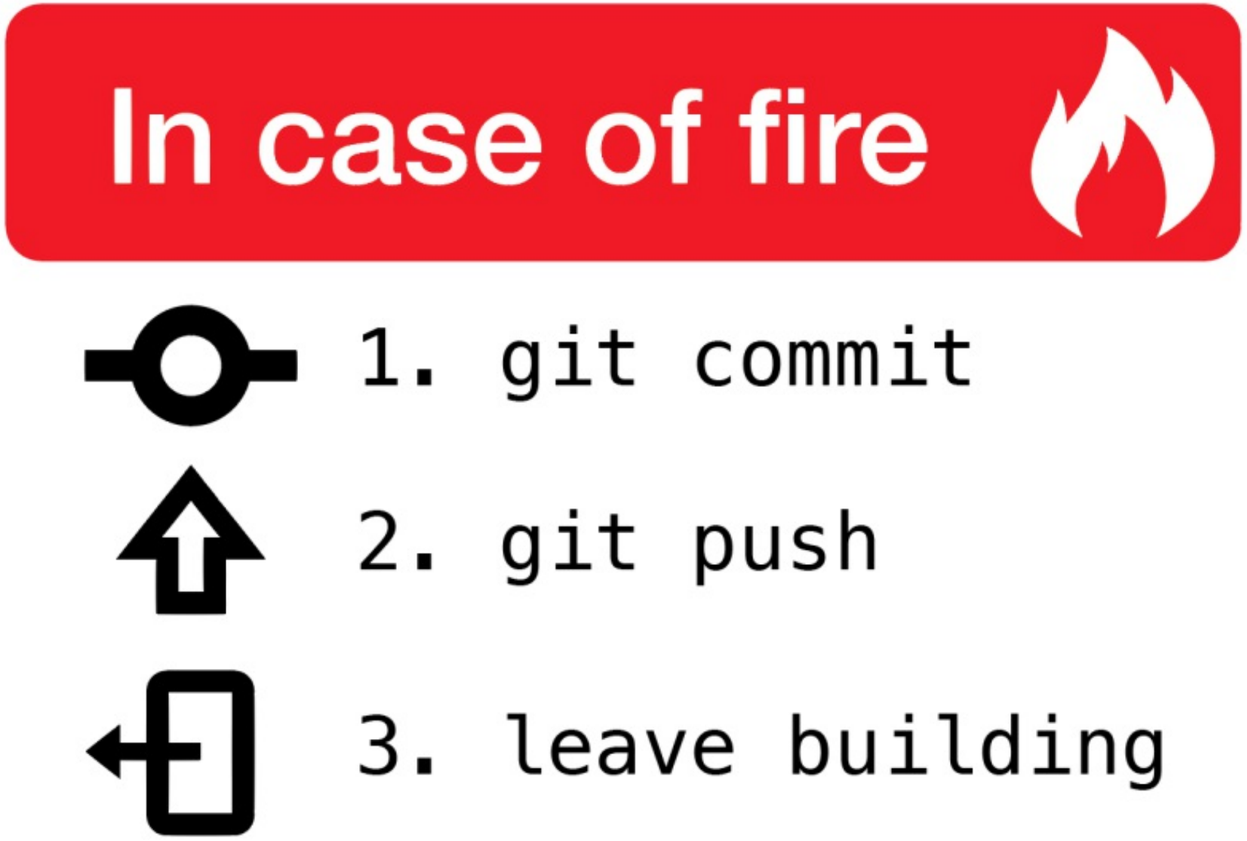
- From Lecture 6
  - `ifconfig enp0s3 | grep 'inet ' | tr -s "[:space:]" ":" | cut -d ":" -f 4`
- From the `Makefile`
  - `cat /var/log/passwords | cut -d';' -f3 | grep -vE '^[[:cntrl:]]|^[[:space:]]*$$' | cut -d= -f2 | tr -d ' ' | sort | uniq | tee -a usernames.txt`

Security

What to do about all these attempts?

- Configure settings in `/etc/ssh/sshd_config` to prevent password based authentication
- fail2ban

Attendance



Questions?