Security Training: Securing SSH Access

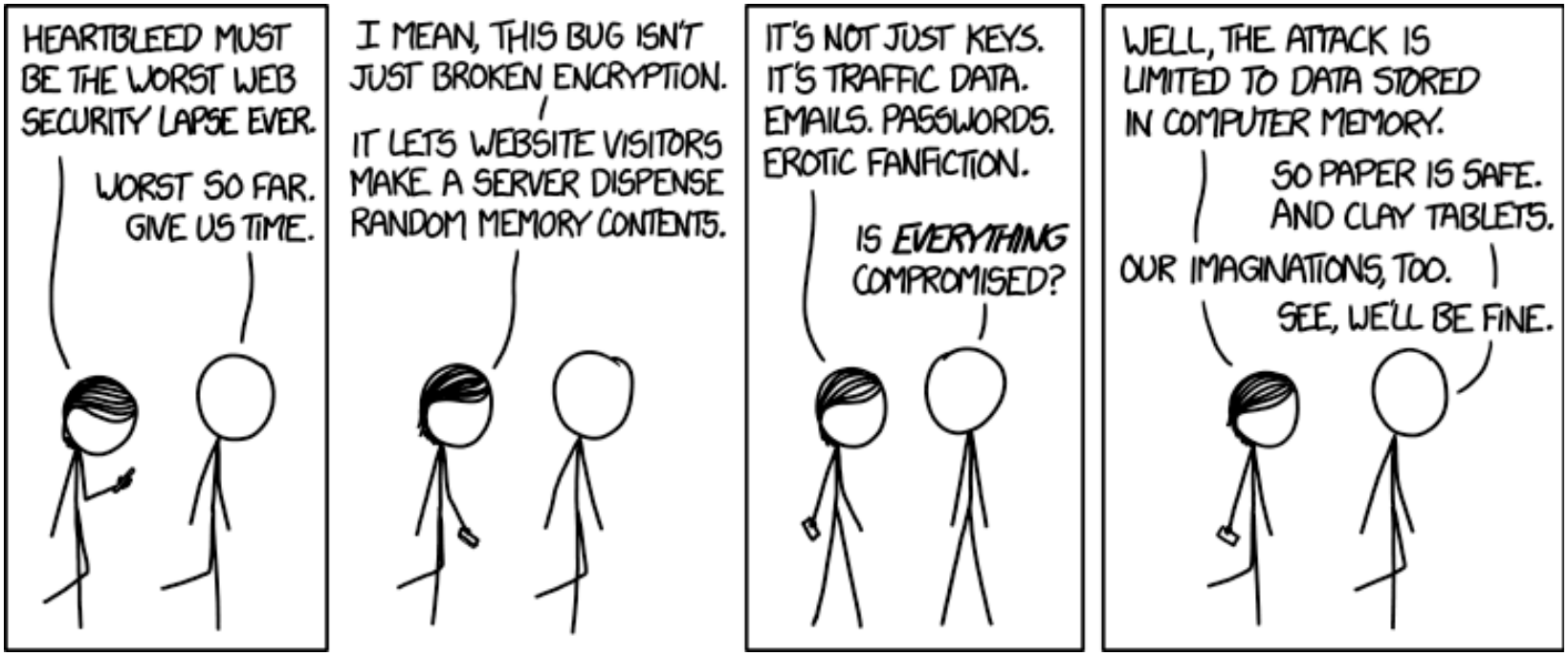
Kevin Hill
OSG Security Team
Fermilab

Open Science Grid

Objective

- Brief overview of OpenSSL/Heartbleed vulnerability.
- Securing SSH
- More passwords mean more problems, here's some help….
- Fail2ban
- 2 factor authentication with Google Authenticator example.

XKCD



Alt text: “I looked at some of the data dumps from vulnerable sites, and it was ... bad. I saw emails, passwords, password hints. SSL keys and session cookies. Important servers brimming with visitor IPs. Attack ships on fire off the shoulder of Orion, c-beams glittering in the dark near the Tannhäuser Gate. I should probably patch OpenSSL.”

OpenSSL/Heartbleed

- A malformed request tricks the server to returning a chunk of its private memory.
- Memory can include the servers private key, and potentially snippets of traffic that was encrypted/ decrypted by the server.
- All affected servers need to be patched ASAP.
- All servers should have certificates replaced with new keys.
- Users of affected services should reset passwords **after** the server is patched and re-keyed.

Securing SSH

- Phishing/Trojan likely source of password compromise these days.
- Bad guys can still use dictionary attacks. Your password isn't in a dictionary is it?
  - Scan system.
  - Look for open services.
  - SSH brute force attack.
  - Other vulnerabilities?

Bad Guy in the System

- Once we are in:
  - Look for other credentials
  - Ssh keys need to have passwords, or attacker will have free access to potentially all the systems in your known_hosts file
  - Start “bad” processes.
  - Scan network further.

Are We Being Attacked?

- Is system acting abnormally?
- Check logs for unusual activity.
- Check for unusual processes.
- Check for unusual network connections.

Report Incident

- Follow OSG procedures to report incident.
- Call GOC, open ticket.
- Disconnect network!

Open Science Grid

Forensics

- Check for running processes.
- Check for odd port usage.

Open Science Grid

Defense

- Block compromised credentials.
- Secure ssh with checklist.
- Configure iptables.
- Configure fail2ban.

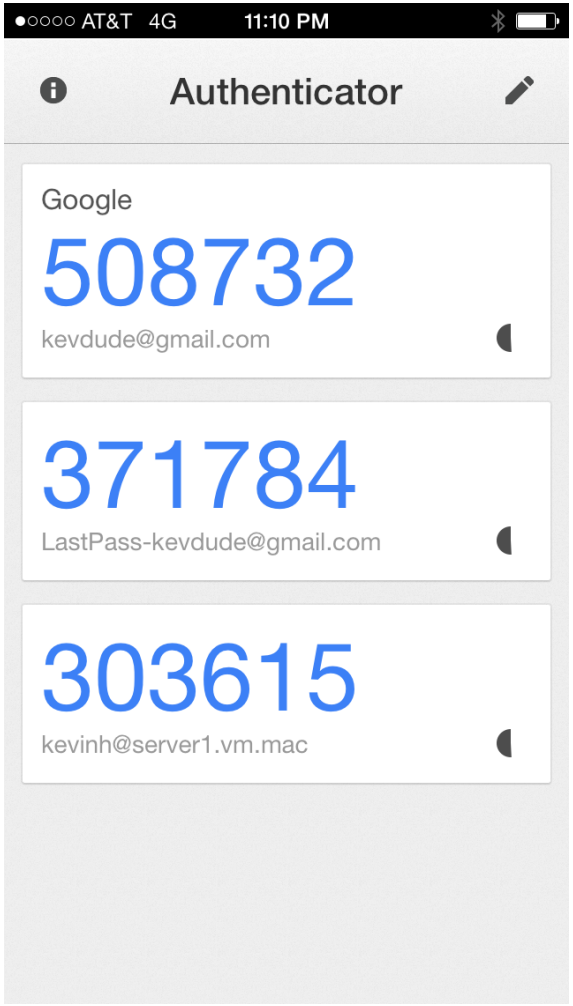
Install Two Factor Auth

- Two factor auth requires both a password you know, as well as a code from a device you have.
- Provides second level of defense after passwords.
- Google Authenticator is free to use, has some limitations in larger installations.

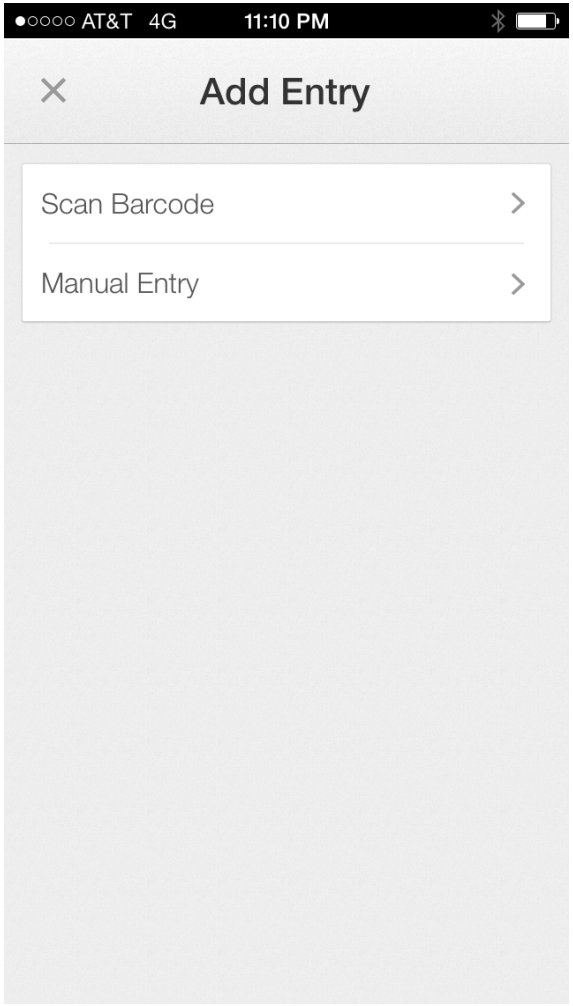
Google Authenticator

- Included in Fedora.
- Get code and compile from code.google.com
- Add to pam.
- Create code and add to mobile app by scanning barcode.

Screenshot 1



Screenshot 2



Open Science Grid

Install fail2ban

- Fail2ban blocks hosts via iptables when it sees a certain number of failed login attempts coming from it.
- Fail2ban available from both RPMForge and EPEL.
- Defaults provide reasonable SSH protection out of the box.
- Demo…

Open Science Grid

SSH Defense

- Turn off SSH!
- Only use ssh v2.
- Limit user access
  - AllowUsers root tom `jerry
  - DenyUsers tom jerry
- Configure Idle timeouts
  - clinetAliveInterval 300
  - ClientAliveCountMax 0
- Disable .rhosts files
  - IgnoreRhosts yes

Ssh options cont.

- Disable Host-Based Authentication
- Disable root Login via SSH
- Enable a Warning Banner
- Firewall SSH Port # 22
- Change SSH Port and Limit IP Binding
  - Port
  - Listen Address
- Use Public Key Based Authentication
- Disable Empty Passwords

Open Science Grid

SSH Defense 2

- Disable Host-based authentication
  - HostBasedAuthentication no
- Disable root Login
  - PermitRootLogin no

Open Science Grid

Questions?