Advanced Workshop Security: Server Hardening

Adam Jenkins

Overview

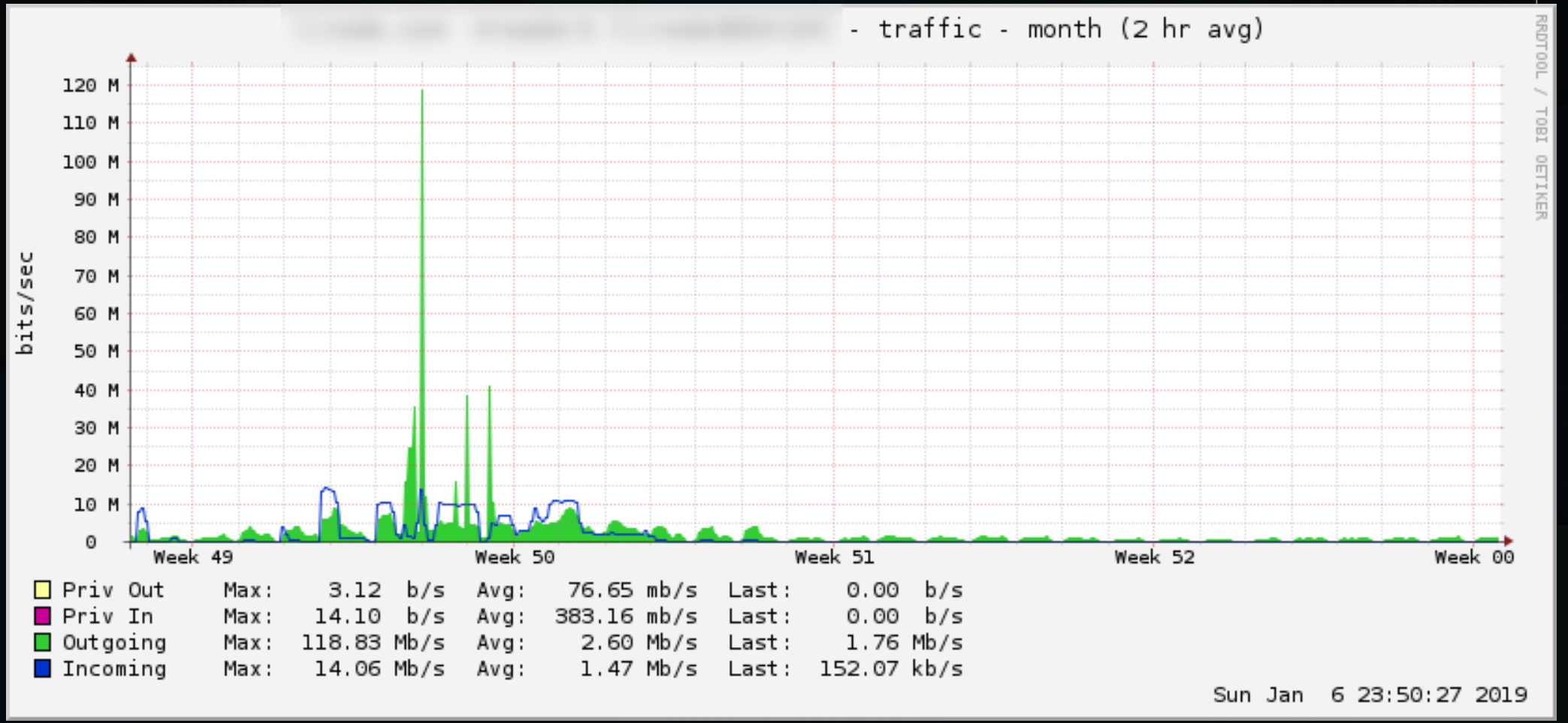
- Security schmecurity… (the WHY)
- TLS with LetsEncrypt (HTTPS – no demo)
- HSTS Headers
- SSH Hardening
- Firewalls with UFW
- Securing the insecure (like PHPMyAdmin)

Security schmecurity

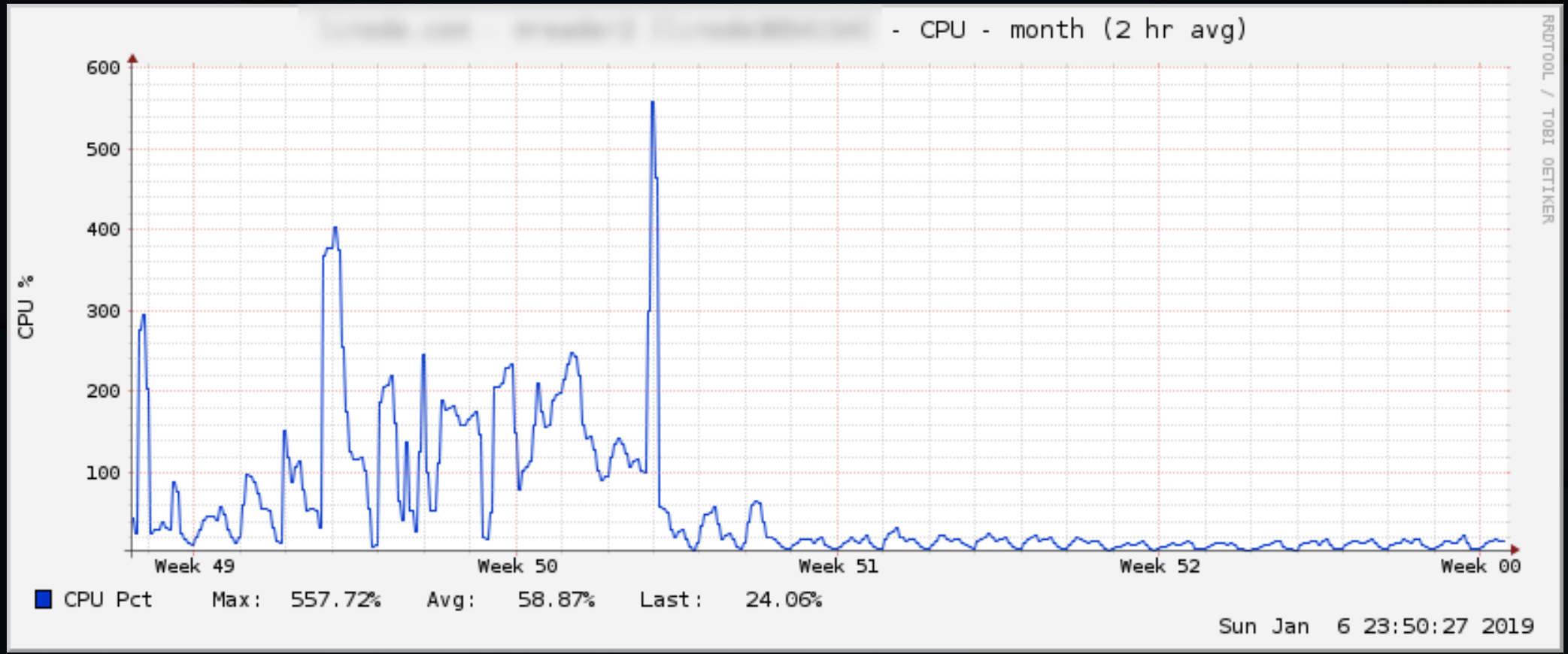
- Improve server performance
- Lessen server load
- Keep the bad guys out

- CIA
  Confidentiality
  Integrity
  Availability

Performance boost, yeah right!?



Performance boost, yeah right!?



Performance boost, WOW!

- Keep the bad guys out leads to:
  - Less network traffic
  - Less CPU load
  - Do more with a smaller server! Save $$$ or ¥¥¥

  So what we want to do is teach our servers to give the bad guys the cold shoulder…

  "Don't waste CPU cycles worrying about that jerk!"

HTTPS

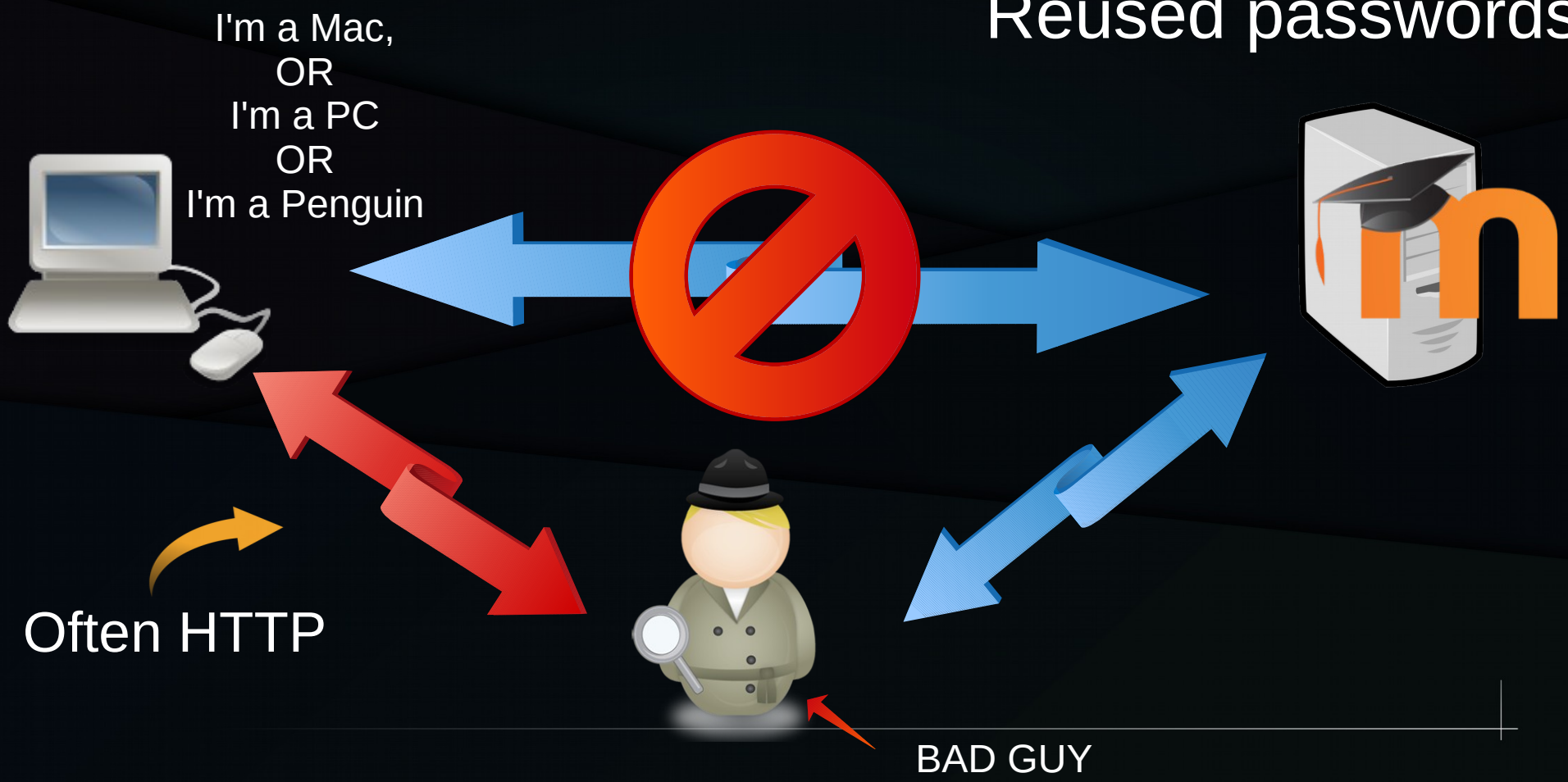
<insert LetsEncrypt Demo here>

http://mootjp19demo.wisecat.net

Why HTTPS?

Man in the Middle (MitM) Attacks

Reused passwords?



HSTS Header

"OK Computer, whenever you connect to me (server), ALWAYS connect using HTTPS. Even if I (or fake me) tell you to connect via unencrypted HTTP, be stubborn and INSIST on HTTPS."

Accept NO substitutes!

```
Header always set Strict-Transport-Security "max-age=63072000;"
```

HSTS Header

63072000 is 2 years in seconds (not the age of Bernie Sanders)

```
Header always set Strict-Transport-Security "max-age=63072000;"
```

Go HARD CORE! – With PRELOAD

Chrome, Firefox and Safari (Edge?? Soon?)

```
...t-Security "max-age=63072000; includeSubDomains; preload"
```

HTTPS and HSTS

- Don't forget to restart the Apache service!

```
sudo service apache2 restart
```

SSH Hardening

- Change the port from 22 to something better
- Do NOT allow root login
- Do NOT allow login using passwords
- KILL the test user (testuser)

`/etc/ssh/sshd_config`

SSH Hardening - commands

```
ssh-keygen
ssh-copy-id ...
```

*/etc/*ssh/sshd_config

SSH Hardening

- Don't forget to restart the SSH service!

```
sudo service ssh restart
```

Firewall

1)Install the firewall

2)Open the ports we need opened (allow)

3)Set a default action (deny)

4)Enable the firewall

NOTICE THE ORDER!

Firewall

```
1) sudo apt install ufw
2) sudo ufw allow 80 (and 443 and 22 etc)
3) sudo ufw default deny
4) sudo ufw enable
```

NOTICE THE ORDER!

Stay secure!