What Your Mother Never Told You About

Automating Security

whoami

Jason Rohwedder

@jasonrohwedder

geek @ Risk I/O

NOT A NEW THING

Security is Hard

Be methodical.

It takes time.

Your App

Continuous Integration

Continuous Deployment

Agile Datacenter

Iterate. Iterate. Iterate.

Production-like development and testing

HOSTING?

Unicorns

Heroku

AppEngine

Datastore-aaS

So Secure Hosting?

Firehost

NETWORKS

Transport security

Physically controlled network

Logically Isolated network - VLAN / VPC

Internal VPN

SSL all the things!

Network Access

host-based firewalls

firewall management apps

AWS - security groups

AWS - VPC subnet ACLs

Host Firewalls!

cookbook: iptables

cookbook: iptables-ng

cookbook: firewall

Auto-Firewall!

cookbook fail2ban

DIY?

WAF - Web App Firewall

stale cookbook: mod_security (sorry)

SaaS: Incapsula

SaaS: darkshield.io

DoS/DDoS Protection

app: bouncer *cookbook soon!*

SaaS: Incapsula

SaaS: prolexic

SaaS: cloudflare

SaaS: darkshield.io

Bastion host

Limited services (eg ssh and vpn)

Use 2-factor!

SSH

Use keys not passwords

cookbook: openssh

cookbook: users

sudo

Do people still use root?

cookbook: sudo

cookbook: users

VPN

cookbook: openvpn

cookbook: users

2-factor

No Excuses!

ssh: cookbook duo-unix

ssh: cookbook other duo-unix

vpn: **TODO!** (okay one excuse)

SERVERS

Software Updates

cookbook: unattended_upgrades *OLD?*

cookbook: apt-periodic

SaaS: cloudpassage

Pin/Freeze critical or unreliable packages

OS Hardening

cookbook: selinux

cookbook: sysctl

IDS-ish

cookbook: snort

cookbook: ossec

cookbook: aide

SaaS: cloudpassage

SaaS: opsmatic *ALPHA*

Encrypting Resting Data

cookbook: encrypyted_volume

cookbook: encryptfs

cookbook: zncrypt

Encrypting Backups

cookbook: encrypted_s3 **TODO!**

cookbook: tarsnap

network volume with encryption

Centralized Logging

cookbook: rsyslog

cookbook: logstash

cookbook: splunk

cookbook: graylog2

SaaS: loggly

TESTING!

Static Analysis

(Ruby on Rails)

rubygem: brakeman

SaaS: code climate

SaaS+app: veracode

Static Analysis

Datacenter?

SaaS: Evident.io

Host Vulnerability Scanning

SaaS: Qualys

App: Nessus

cookbook: nessus

WebApp Vulnerability Scanning

SaaS: Whitehat Sentinel

SaaS: Qualys WAS

Fixing things!

(you knew it was coming)

SaaS: Risk I/O

WarGames!

MOAR?

@jasonrohwedder

https://github.com/jro/automated_security
HELP!

https://github.com/risk-io

https://github.com/HoneyApps/chef-mod_security

T-shirts?

bug bounty

pull requests

non-chef branches of WarGames