Top 10 Security Practices for Protecting Your Infrastructure

@masonegger

Mason Egger
Developer Advocate

@masonegger

https://mason.dev

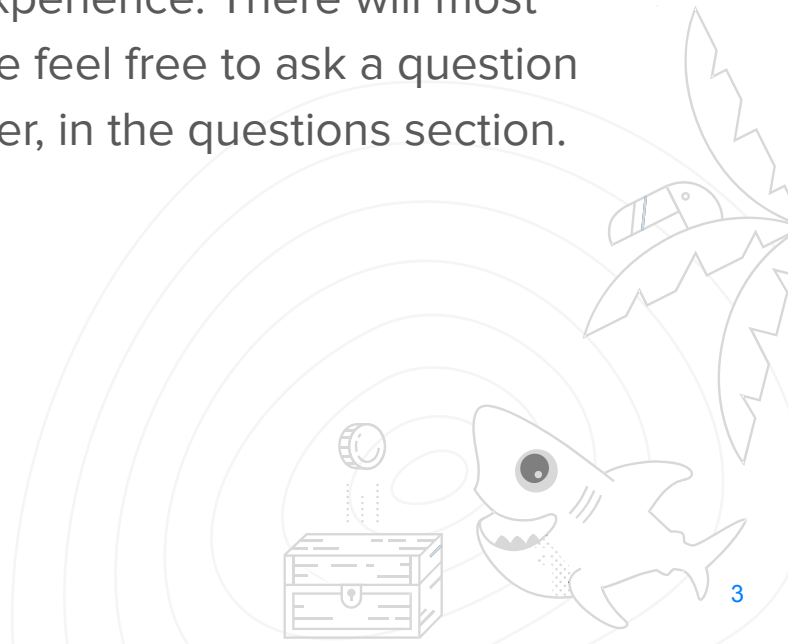
mason@do.co

https://twitch.tv/codingwithmason

Goals of the Webinar

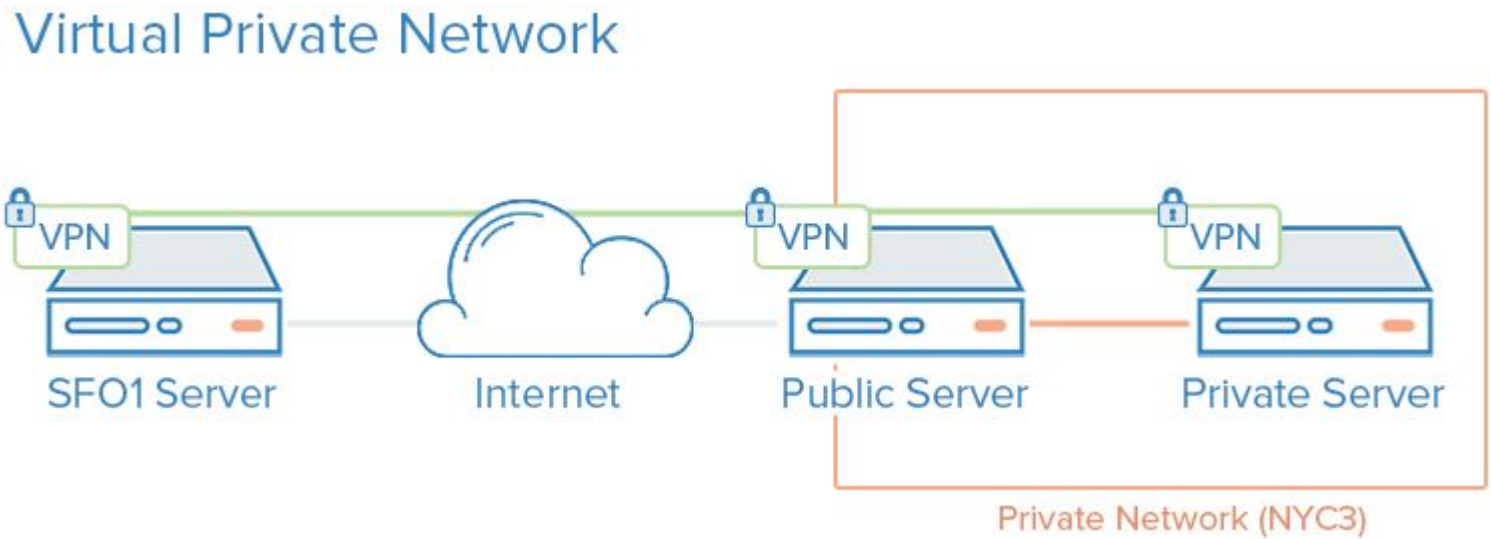
- To inform you of what I consider the most crucial, *minimal set* of tasks to minimize your chance of compromise

- These are my opinions based on my experience. There will most doubtedly be something left out. Please feel free to ask a question about any topic, not just the ones I cover, in the questions section.



Tip #10 - Use VPNs

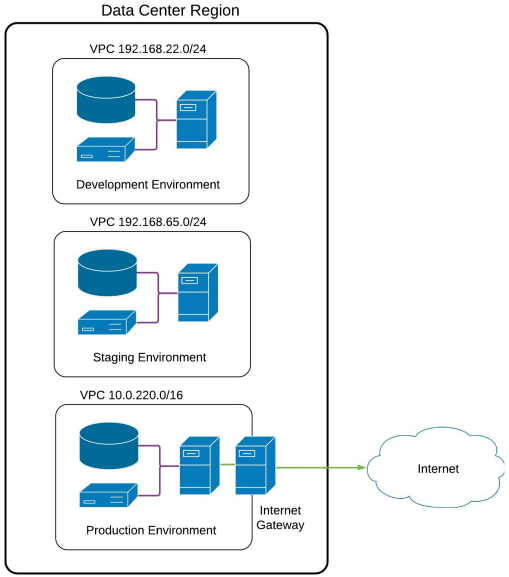
- Can purchase or setup yourself
- Examples: Wireguard, OpenVPN, OpenConnect, Tinc



Tip #9 - VPCs and Isolated Networks

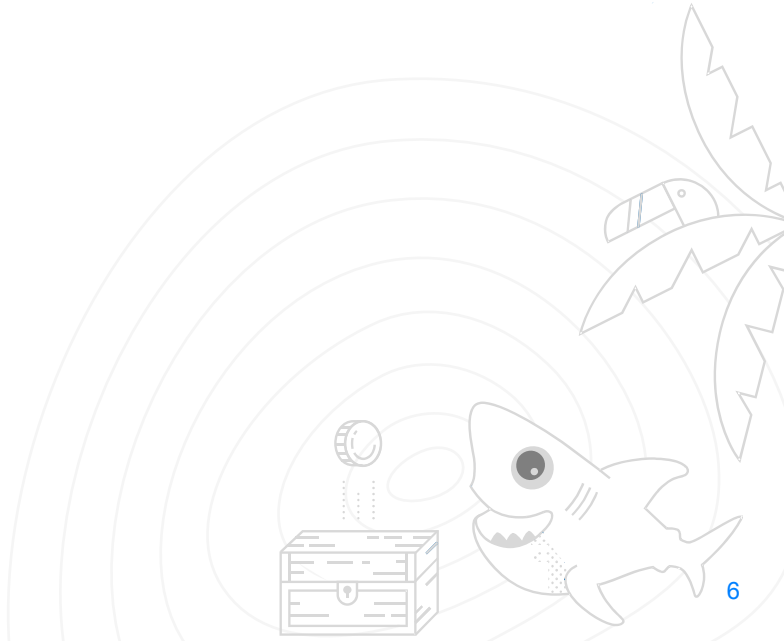
- Virtual Private Cloud

- Isolate networks, such as prod, dev, stage, from each other and the rest of the company



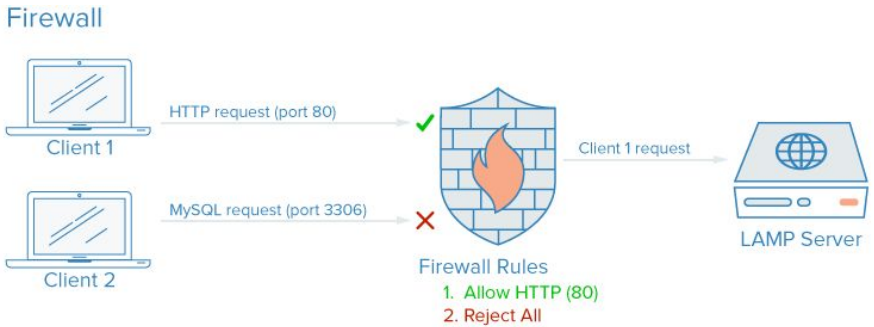
Tip #8 - Keep Your Software Updated

- The longer a bug exists in the wild, the more likely it will be found
- Keeping software up to date on servers and personal machines minimizes compromise
- `sudo apt install unattended-upgrades`



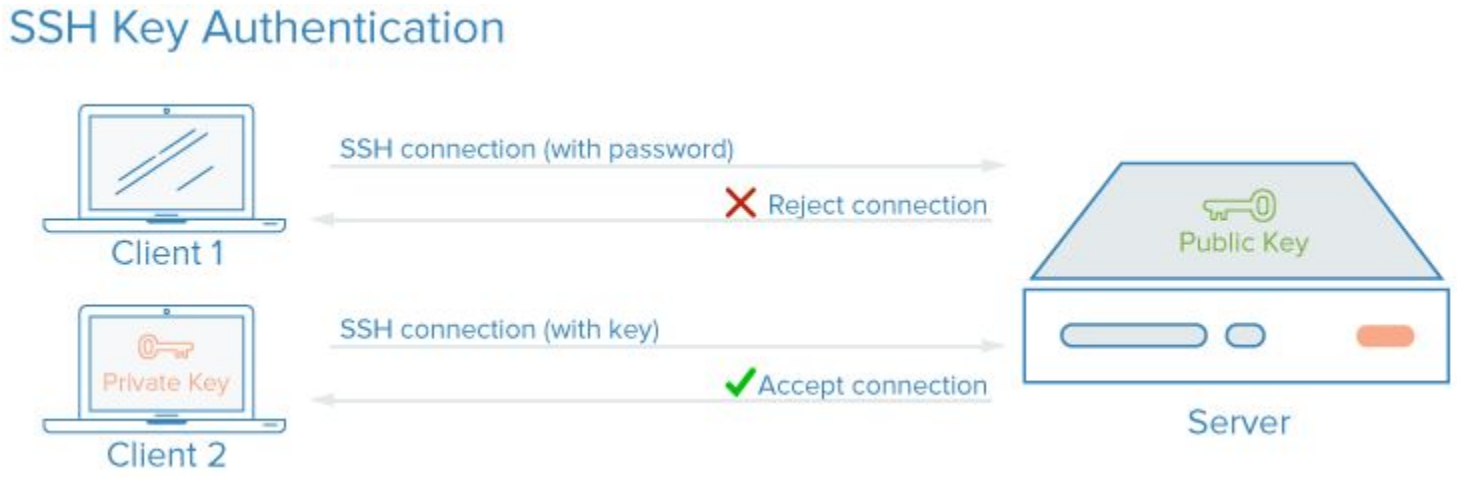
Tip #7 - Use Firewalls

- Use both external and internal firewalls
  - Cloud provider and OS
- Regulate traffic *to* your servers and *between* your servers



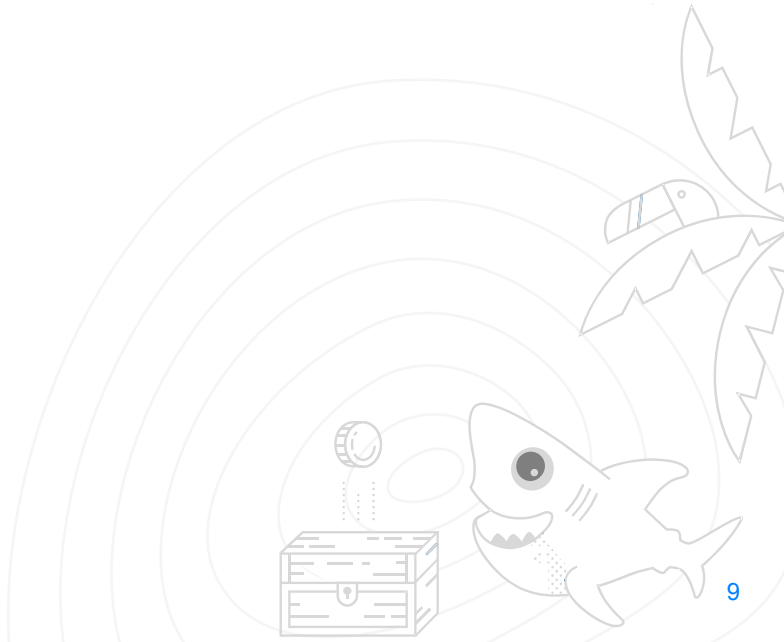
Tip #6 - Key Based Authentication

- Do not allow password based authentication if you can avoid it
  - SSH
- SSH Keys tend to be more bits and built on strong encryption algorithms, making compromise nearly impossible



Tip #5 - Establish a Zero Trust Network

- Just because you're on the network doesn't mean you should be trusted
- Don't be a castle with a moat
- Multi Factor Authentication is a *must*

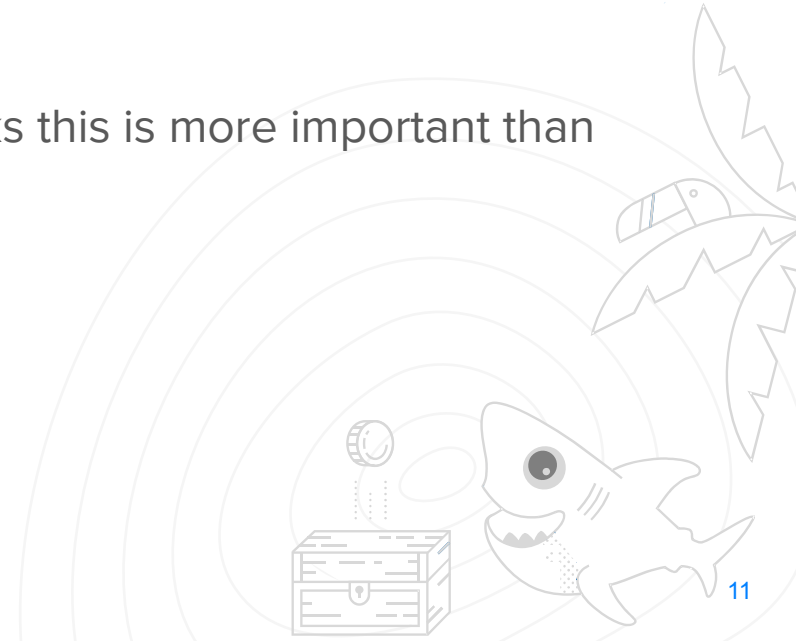


Tip #4 - Establish the Principle of Least Privilege

- No one should be able to ssh directly in as root
- If you don't need access, you don't get access
- *sudo* can serve both as a gating mechanism and an intrusion detection system
  - You need to be able to audit who did what on your system.
- This applies to applications and APIs also, not just users

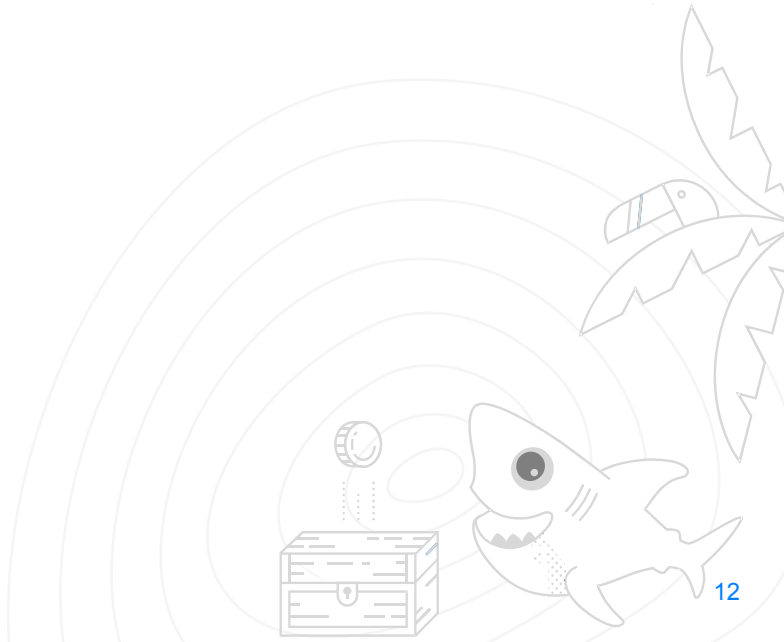
Tip #3 - Have backups, both on and off site

- A backup that’s never been restored isn’t a backup, it’s a prayer
- Do not rely on a single entity to take care of all of your backups. That is a single point of failure
- With the advent of Ransomware attacks this is more important than ever



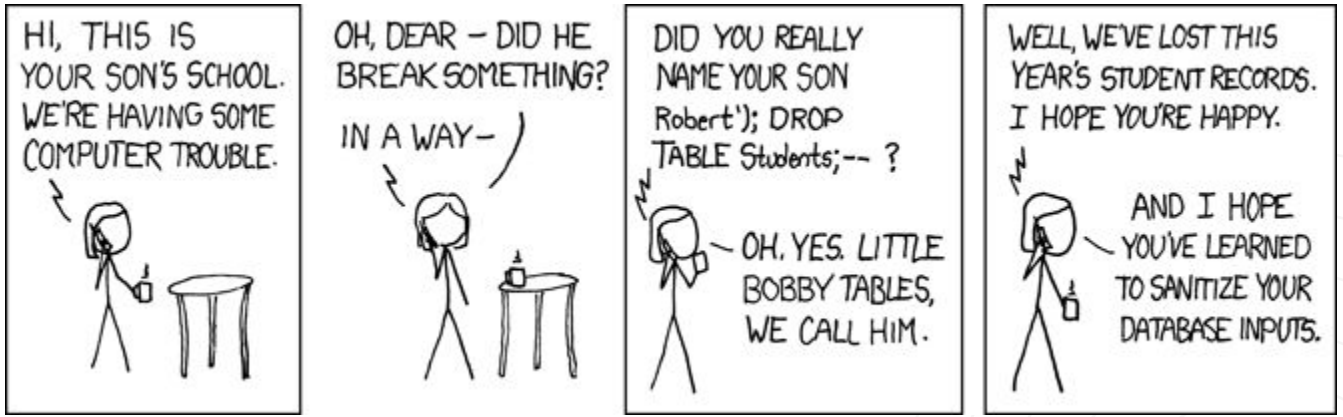
Tip #2 - Audit Your Services

- “It’s 10:00, do you know what’s running on your server?”
- Lack of auditing is how botnets and crypto miners go undetected
- `sudo ss -plunt`



Tip #1 - Sanitize Your Inputs

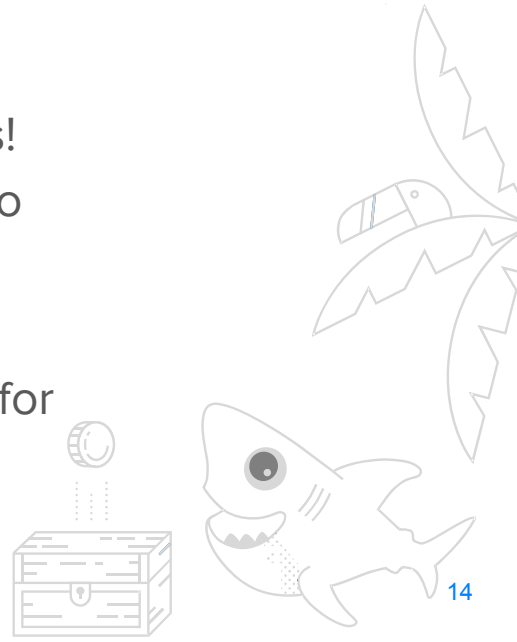
- “Always assume the person on the other end of your site is a malicious jerk trying to steal your kittens” - my mentor



source

That's all for this time!

- Be sure to be on the lookout for more DigitalOcean webinars/workshops like this!
- Tune in every last Thursday of the month to watch more of my webinars
- Hacktoberfest ends Saturday!
- Try out DigitalOcean with $100 free credit for 60 days with https://do.co/mason



Mason Egger

Developer Advocate
DigitalOcean

do.co/deploy

Tue, Nov 10 - Wed, Nov 11
10:00a.m. EDT

Register

deploy
by DigitalOcean