Crypto.com Mainnet Dry-run - Crossfire Security Checklist

Part 1 - Conduct Survey on General Controls of Hosting Data Centre

Description: Perform a survey on the hosting data centre, and compare your result with the best practice below

Controls Category	Description of Best Practice	Survey Result
Data Center	Your hosting data centre should have following features	
	- Redundant Power	
	- Redundant Cooling	
	- Redundant Networking	
	- Physical Cage/Gated Access	
	- Remote Alerting Security Camera	

Part 2 - Current Status of Node Setup

Description: Run the checking script with following steps, and also manually inspect system configuration. Then compare your result with the best practice below.

- Download the audit script file zip from https://drive.google.com/file/d/1FA2ZfVrKo1Pe55m37x9EiyRZSZzj6jt6/view?usp=sharing
- Check the sha256 sum of the zip file

```
echo "d6b00eb881037100d2ce77eaa27aae3537c3fcdadb655208f09b53e914e2a632 audit-script.tar.xz" | sha256sum -c
```

- Unzip the file

```
tar -xf audit-script.tar.xz
```

- Run the audit script file

```
./audit-script -l
```

Controls Category	Description of Best Practice	Survey Result
General System Security	Operating system appropriately patched. Kernel is updated to latest stable version. The node should be operated in x86_64 environment	
	Auto-updates for operation system is configured. Toolkit for automatic upgrades exists (e.g. auter, yum-cron, dnf-automatic, unattended-upgrades)	
	Security framework enabled and enforcing. SELinux | AppArmor | Tomoyo | Grsecurity Enabled.	
	No insecure and unnecessary services Installed. (e.g. telnet, rsh, inetd, etc ...)	
	GRUB boot loader password is configured. Grub2 configured with password	
	Only root permissions on core system files	
Mainnet related File Directory Security	Secure the directory "~/.chain-maind" to be accessible by owner only	

Mainnet Binary Configuration	Recommed the following settings in config.toml for both performance and security
	For sentry nodes:
	max_num_inbound_peers = 500
	max_num_outbound_peers = 50
	flush_throttle_timeout = "300ms"
	For validator node:
	max_num_inbound_peers = 100
	max_num_outbound_peers = 10
	flush_throttle_timeout = "100ms"	

	Following Pasword policies are enforeced: - No Blank Passwords - Weak Passwords Not Allowed	

Account Security & Remote Access	Following SSH configurations are enabled: - PermitRootLogin no - PasswordAuthentication no - ChallengeResponseAuthentication no - UsePAM yes - AllowUsers <Neccesary user only> - AllowGroups <Neccesary group only>	
Networking	Network throughput test using speedtest. Recommend to have at least 5 Mbps upload, 5 Mbps download)	
	Host-based (e.g. iptables) or cloud-based (e.g. AWS Security Group) firewall is enabled to protect all the involved nodes. Remote management ports (e.g. SSH - TCP 22) should only be exposed to selected IP instead of the internet. No overly permissive rules (e.g. wide range of allowed ports 1-65535) should be set. For internal communication channels between nodes, they should be set with specific source and destination addresses. For internet reachable nodes, set TCP 26656 to be the only incoming port, if possible.	
	Intrusion Detection / Prevention System (e.g. Fail2Ban, Snort, OSSEC) is installed and enforcing	
	Setup sentry node architecture to protect validator node, and set firewall rules to restrict direct internet access to it.	
Redundancy	Hot standby node is setup with the same configuration as main node	
	System monitoring and alerting is setup to alert owners on anormalies	
Key Managment	Setup Tendermint KMS with HSM or equivalent online service, which should replace the static key file.	
DDOS	Setup validator in accordance with sentry architecture. Setup instruction: https://docs.tendermint.com/master/nodes/validators.html#setting-up-a-validator Detailed description: https://forum.cosmos.network/t/sentry-node-architecture-overview/454	