Infrastructure Cyber Defense

Project details

Welcome to **Powerzio**, the leading energy company in the world.

We are proud to announce that we are now offering a new service to our customers: *Powerzio Home*.

This service will allow our customers to monitor their energy consumption in real time, and to control their devices remotely.

In order to provide this service, we need to build a new infrastructure, our old one seems a bit compromised.

As a security engineer, you have been asked to design this infrastructure and to monitor our currently hacked machine.

You'll find all details in the next pages.

Welcome on board,
Powerzio Team

I - Hosting

We'll need to have a new machine running on our infrastructure with the following requirements:

Requirement	Details
Resources Monitoring	We need to monitor the CPU, RAM and Disk usage of the machine.
Backup Strategy	We need to backup the machine regularly, provide documentation and scripts
Spam Filtering	You'll need to detect flooding on the HTTP Server and provide temporary bans (30 seconds). Also you need to create a way to filter traffic coming from specific IPs
VPN Link	We have other machines running on our infrastructures and we want you to create a link to them using a VPN. You'll receive Wireguard credentials. This uplink should restart upon machine restart
Infected machine audit	We need you to have a look at one of our machines, it seems to have been infected somehow, write a report to explain when/how/by whom.
Infected machine remediation advice	In your report, include advice in the way we can make this machine more secure and resilient.
Bank App	Deploy the bank application (bank.powerzio.net) and expose it on port 443
Bank app code audit	Have a look at the bank application's code, **without changing anything in the code** note the vulnerabilities you notice there.
Bank app audit remediation	Using a **WAF** or any kind of firewall, fix as well as you can the vulnerabilities you noticed in this web application. **as a reminder, do not edit the code directly** but use **firewall rules** instead.
DNS Rules	Please host a DNS service with the additional following entries : CNAME f -> files.powerzio.net, CNAME beta-f -> beta.files.powerzio.net. 'A' link of 'g' to 8.8.8.8 TXT record of dev to "hello world" bank.powerzio.net should point correctly to the web application.
HTTPS Documents Exposure	You need to hosts your audit reports as static documents at files.powerzio.net (HTTPS)
SSH Access	You need to expose a SSH service for the **powerzio** user with **sudo** permissions. Also, to spice things up, password authentification must be turned on and the associated password must be part of this list. You will be provided a **SSH public key** to add to this server.

II - Audit

We need you to have a look at an infected machine, credentials will come in your mail.

To access the machine you'll use Wireguard.
We expect you to explain what you found and how did this happen, you will need to write a small text report with your findings.

Length should be around 1 page maximum.

Also, please provide remediation steps for **us** to fix the machine, do not fix it on your end.

How to turn in?

You'll need to create a **private** Github repository and to invite lp1Dev and MikkLfr

During the delivery part, we'll launch command against your hosted machine through the VPN uplink, you'll need to have the machine up and ready.

Questions?

Please ask any questions through Teams to Jeremie1.Amsellem **and** Michael1.Ohayon