HTTP and HTTPS MitM Apache Reverse Proxy

Security questions

explain the steps above. Explain what you did

1. Step: clonening the repo from gihtub to the local maschine
   The config files containts the reverse proxy settings, currently point to the locahost backend system
2. Step: Building the docker service an testing the http and https port for reachability
3. Step: Changeing the reverse proxy config, especelly this is relevant for the given configuration

```
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off

<Location />
    ProxyPass https://pwspray.vm.vuln.land/
    ProxyPassReverse https://pwspray.vm.vuln.land/
</Location>
```

explain the benefit of having a http to https reverse proxy

The attacker don't have to distribute asymmetric keys or take over a PKI system, the main benefit is the use don't receive any notification from the browser and this could also be a drawback for a user

explain the benefit of having a https to https reverse proxy

The benefit is the use has the impression to be on a real site and don't have any consideriation to be part of a MitM attack. The setup is therefore more complex but with higher chance of successfull attack.

explain how your reverse proxy online phishing could be advertised to a victim

- within the same network (LAN)
    - Rouge DHCP
    - ARP request spoofing
    - DNS server take over
    - mDNS spoofing
    - DNS spoofing
    - Router take over
    - Packet injection
    - Swtich take over
- over the internet
    - Phishing Email

    - Whaling
    - DNS Cache poisoning
    - DNS spoofing
    - Attack againt routing protocols such as BGP, iBGP, eBGP, etc.
    - DNS Spoofing against routers or DNS server in a LAN

- in public

    - QR codes