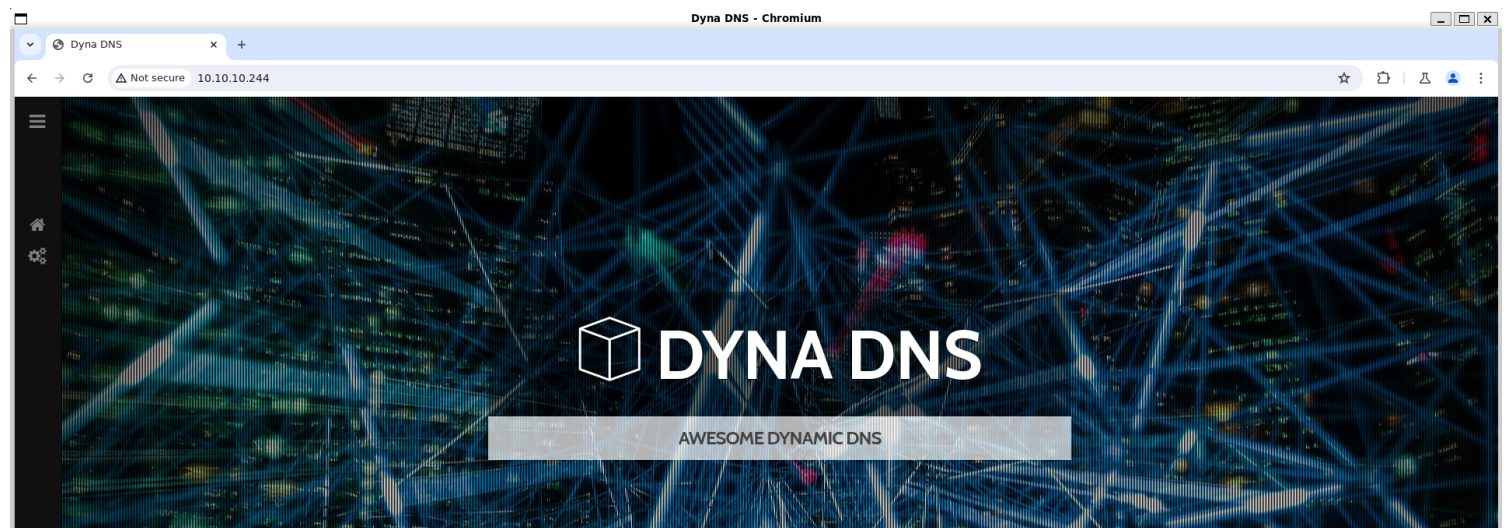


# Information Gathering

## 1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ tcpscan 10.10.10.244  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 19:03 IST  
Nmap scan report for 10.10.10.244  
Host is up (0.20s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|_   3072 05:7c:5e:b1:83:f9:4f:ae:2f:08:e1:33:ff:f5:83:9e (RSA)  
|_   256 3f:73:b4:95:72:ca:5e:33:f6:8a:8f:46:cf:43:35:b9 (ECDSA)  
|_   256 cc:0a:41:b7:a1:9a:43:da:1b:68:f5:2a:f8:2a:75:2c (ED25519)  
53/tcp    open  domain   ISC BIND 9.16.1 (Ubuntu Linux)  
|_ dns-nsid:  
|_   bind.version: 9.16.1-Ubuntu  
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))  
|_ _http-title: Dyna DNS  
|_ _http-server-header: Apache/2.4.41 (Ubuntu)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 81.93 seconds  
  
vigneswar@VigneswarPC: ~  
$
```

## 2) Checked the website



## 3) Enumerated the dns

```
(vigneswar@VigneswarPC)-[~]
$ dig ANY -x 10.10.10.244 @10.10.10.244

; <<>> DiG 9.19.21-1-Debian <<>> ANY -x 10.10.10.244 @10.10.10.244
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61015
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c78a266fb8d067f20100000066f6b53a7b987a2d4a292c48 (good)
;; QUESTION SECTION:
;244.10.10.10.in-addr.arpa.      IN      ANY


;; AUTHORITY SECTION:
10.in-addr.arpa.      60      IN      SOA     dns1.dyna.htb. hostmaster.dyna.htb. 2021030302 21600 3600 604800 60

;; Query time: 189 msec
;; SERVER: 10.10.10.244#53(10.10.10.244) (TCP)
;; WHEN: Fri Sep 27 19:08:02 IST 2024
;; MSG SIZE rcvd: 157
```

#### 4) Found a credentials


### Our Services

She evil face fine calm have now. Separate screened he outweigh of distance landlord.



#### Quality Dynamic DNS


We are providing dynamic DNS for anyone with the same API as no-ip.com has. Maintaining API conformance helps make clients work properly.



#### Awesome Domains

We are providing Dynamic DNS for a number of domains:

- dnsalias.htb
- dynamicdns.htb
- no-ip.htb



#### Beta

We are still running in beta mode. Please use following shared credentials:

- Username: dynadns
- Password: sndanyd

dynadns:sndanyd

#### 5) Checked the api

Dynamic updates are performed by making an HTTP request to one of the following URLs:

`http://dynupdate.no-ip.com/nic/update`  
---  
`https://dynupdate.no-ip.com/nic/update`

For update requests on HTTP, our interface listens on Ports 80 and 8245. Port 8245 is used to bypass HTTP proxies. If updating over HTTPS, our system listens on Port 443 It is not necessary to open any incoming ports for updating.

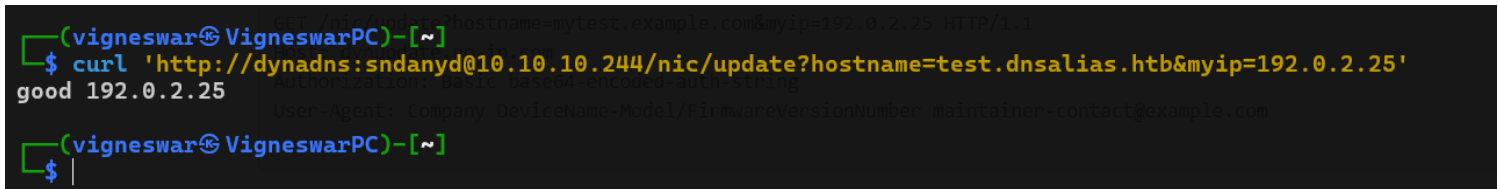
**Authorization:** base64-encoded-auth-string should be the **base64 encoding** of username:password.

**username:password:** Username and password associated with the hostnames that are to be updated. No-IP uses an email address as the username. Email addresses will be no longer than 50 characters. If using group username, our protocol uses special characters. Be sure that special characters can be accepted by your client.  
An example update request string

```
http://username:password@dynupdate.no-ip.com/nic/update?hostname=mytest.example.com&myip=192.0.2.25
```

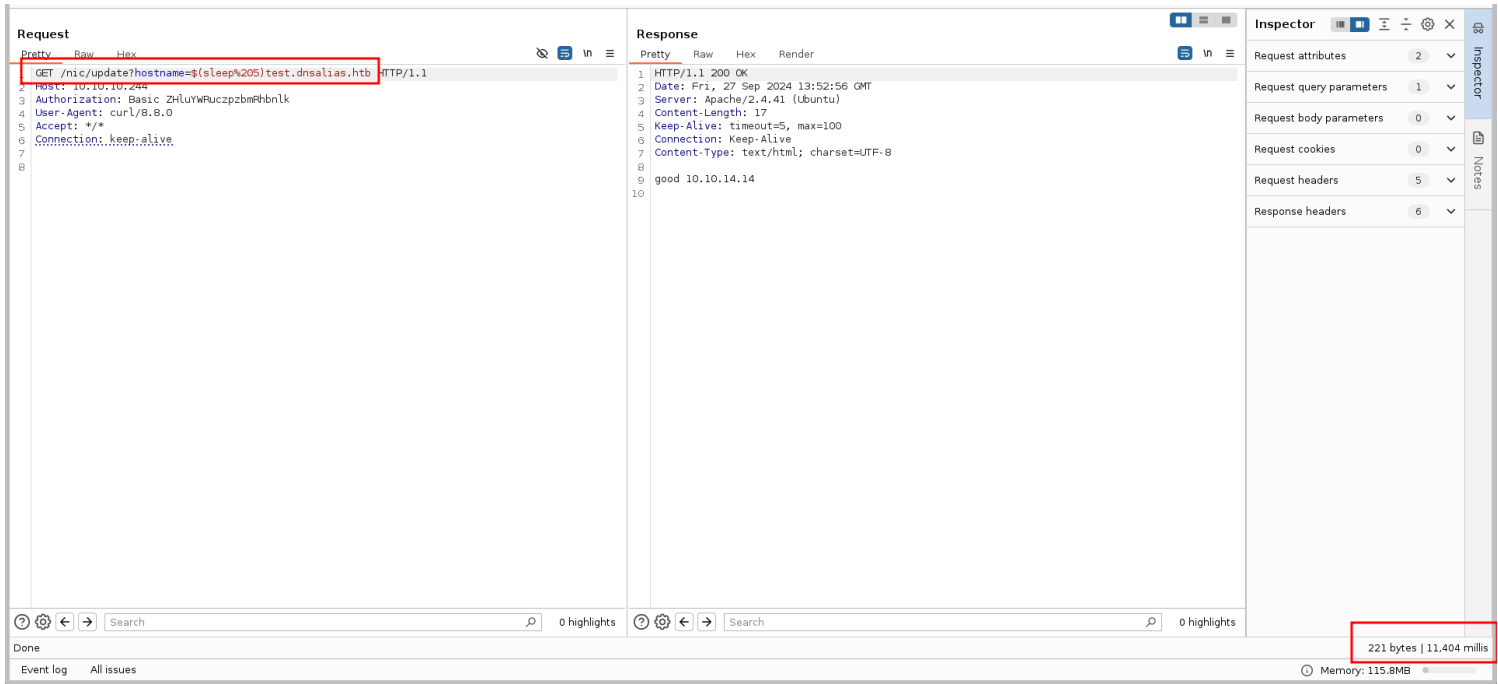
An example basic, raw HTTP header GET request

```
GET /nic/update?hostname=mytest.example.com&myip=192.0.2.25 HTTP/1.1
Host: dynupdate.no-ip.com
Authorization: Basic base64-encoded-auth-string
User-Agent: Company DeviceName-Model/FirmwareVersionNumber maintainer-contact@example.com
```



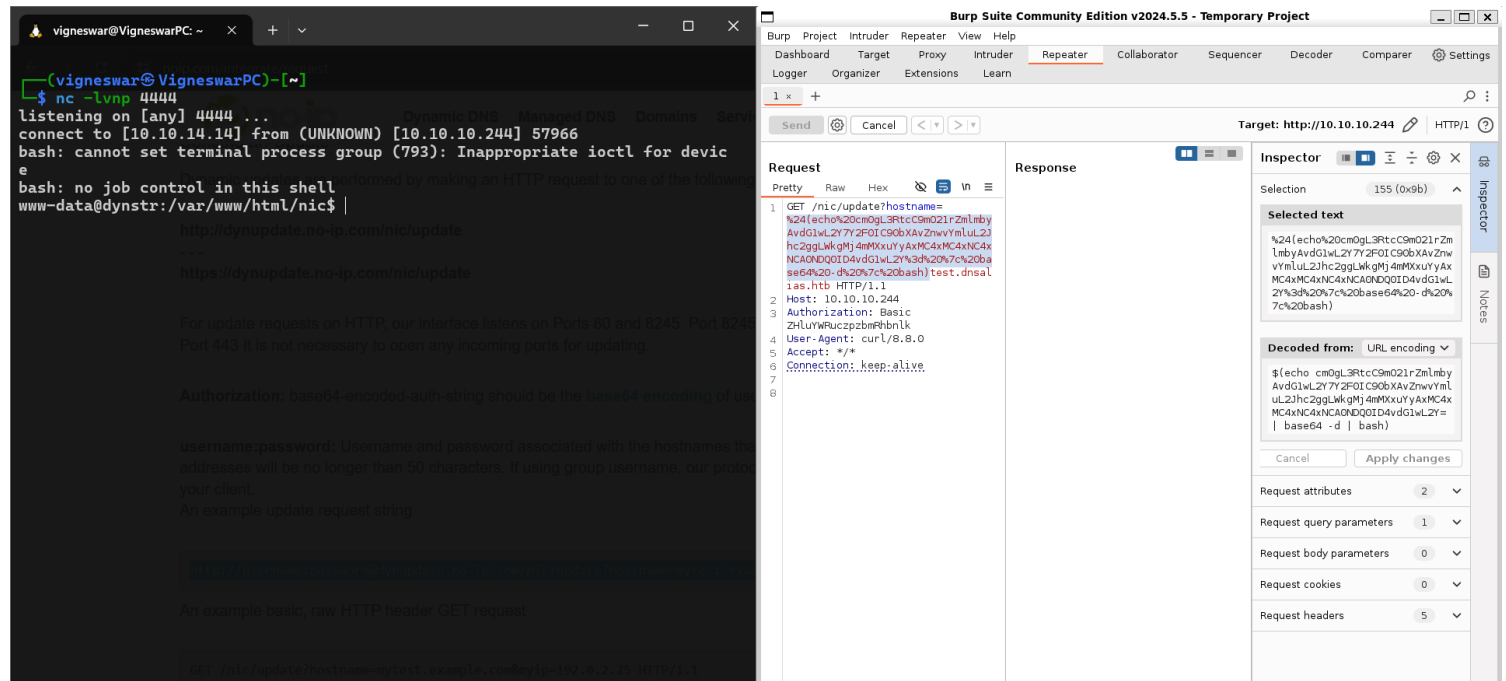
# Vulnerability Assessment

## 1) Found command injection



## Exploitation

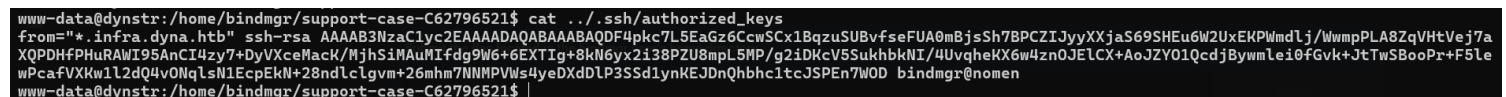
## 1) Got reverse shell



## 2) Found ssh key in a debug output file



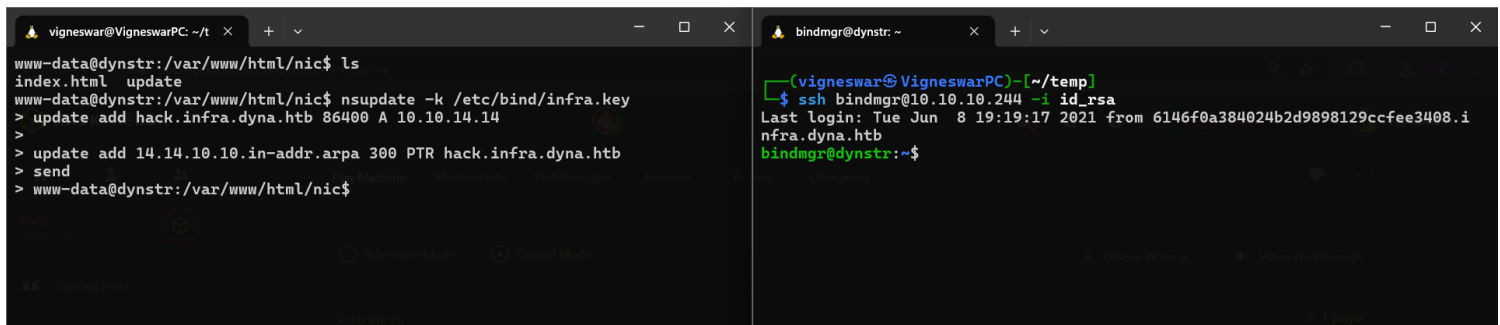
3) We are allowed to login only from particular subdomain



4) Added a dns record

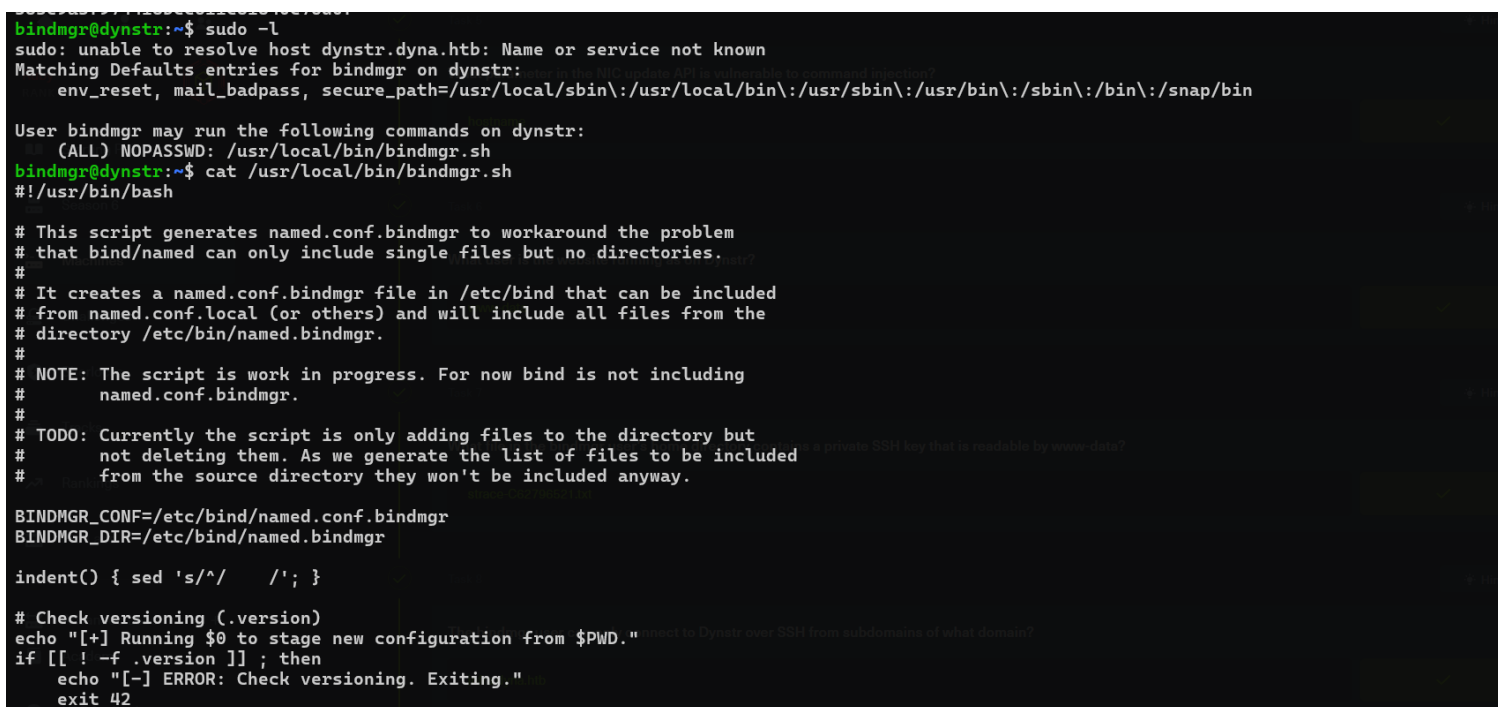
```
nsupdate -k /etc/bind/infra.key
update add hack.infra.dyna.htb 86400 A 10.10.14.14
```

```
update add 14.14.10.10.in-addr.arpa 300 PTR hack.infra.dyna.htb
send
```

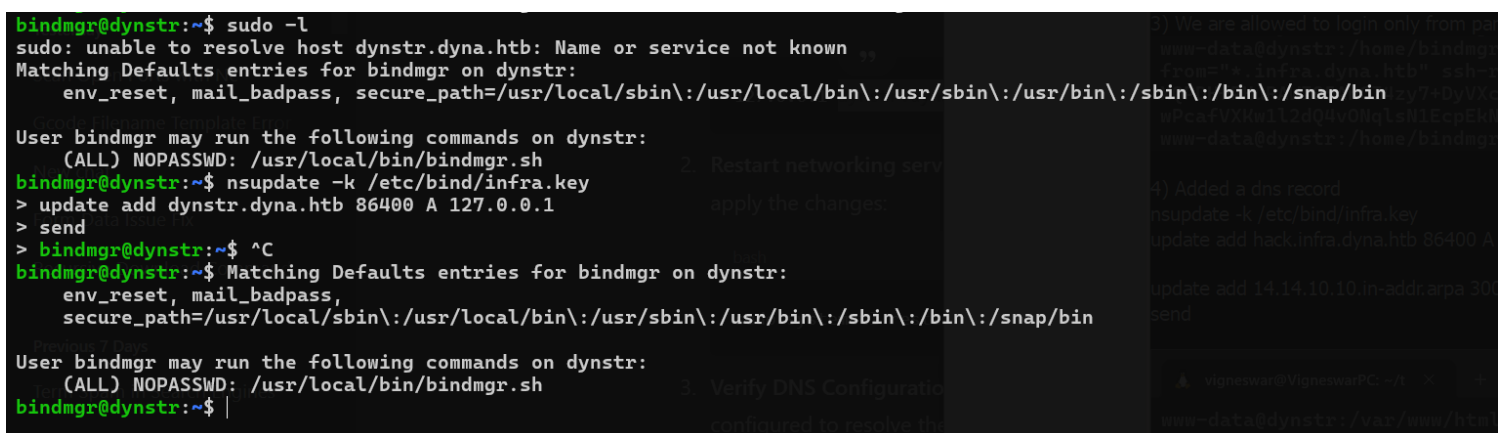


# Privilege Escalation

## 1) Found a sudo permission



## 2) Fixed sudo



## 3) Found a glob vulnerability





```

# This script generates named.conf.bindmgr to workaround the problem
# that bind/named can only include single files but no directories.
#
# It creates a named.conf.bindmgr file in /etc/bind that can be included
# from named.conf.local (or others) and will include all files from the
# directory /etc/bin/named.bindmgr.
#
# NOTE: The script is work in progress. For now bind is not including
#       named.conf.bindmgr.
#
# TODO: Currently the script is only adding files to the directory but
#       not deleting them. As we generate the list of files to be included
#       from the source directory they won't be included anyway.

BINDMGR_CONF=/etc/bind/named.conf.bindmgr
BINDMGR_DIR=/etc/bind/named.bindmgr

indent() { sed 's/^/    /'; }

# Check versioning (.version)
echo "[+] Running $0 to stage new configuration from $PWD."
if [[ ! -f .version ]] ; then
    echo "[-] ERROR: Check versioning. Exiting."
    exit 42
fi
if [[ "`cat .version 2>/dev/null`" -le "`cat $BINDMGR_DIR/.version 2>/dev/
null`" ]] ; then
    echo "[-] ERROR: Check versioning. Exiting."
    exit 43
fi

# Create config file that includes all files from named.bindmgr.
echo "[+] Creating $BINDMGR_CONF file."
printf '// Automatically generated file. Do not modify manually.\n' >
$BINDMGR_CONF
for file in * ; do
    printf 'include "/etc/bind/named.bindmgr/%s";\n' "$file" >> $BINDMGR_CONF
done

# Stage new version of configuration files.
echo "[+] Staging files to $BINDMGR_DIR."
cp .version * /etc/bind/named.bindmgr/

# Check generated configuration with named-checkconf.
echo "[+] Checking staged configuration."
named-checkconf $BINDMGR_CONF >/dev/null
if [[ $? -ne 0 ]] ; then
    echo "[-] ERROR: The generated configuration is not valid. Please fix
following errors: "
    named-checkconf $BINDMGR_CONF 2>&1 | indent
    exit 44
else
    echo "[+] Configuration successfully staged."
    # *** TODO *** Uncomment restart once we are live.
    # systemctl restart bind9
    if [[ $? -ne 0 ]] ; then
        echo "[-] Restart of bind9 via systemctl failed. Please check logfile:
"
        systemctl status bind9
    else
        echo "[+] Restart of bind9 via systemctl succeeded."
    fi
fi

```

