enumeration

nmap -sC -sV -sT -oN /home/kali/machines/retired/bucket/nmap.txt 10.10.10.212
Starting Nmap 7.91 (https://nmap.org) at 2021-05-04 01:57 EDT
Nmap scan report for 10.10.10.212
Host is up (0.30s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open http   Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://bucket.htb/
Service Info: Host: 127.0.1.1; 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 51.51 seconds

here is the result of normal nmap lets run the vuln script and complete tcp scan

vuln script found nothing

nothing on full system scan

running the nmap scan

22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4

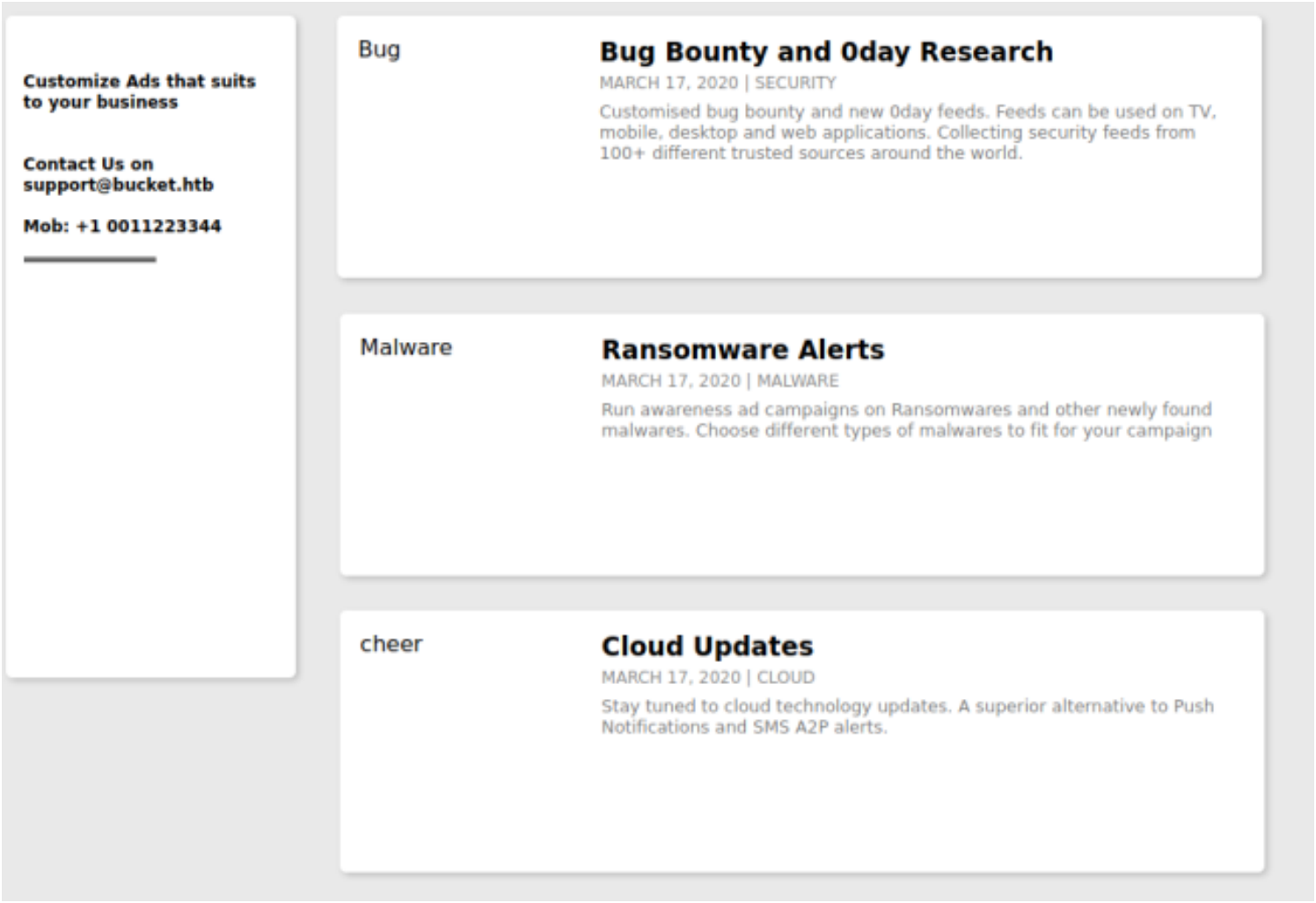
80/tcp open http   Apache httpd 2.4.41

http://bucket.htb/

and a domain name is leaked

lets see if it has domain based routing

it did had domain based rounting so we are on the home page



we see a email support@bucket.htb lets also add it to host file and visit there

nothing the same page now lets bush around the page and we fing nothing just a static page lets run gobuster

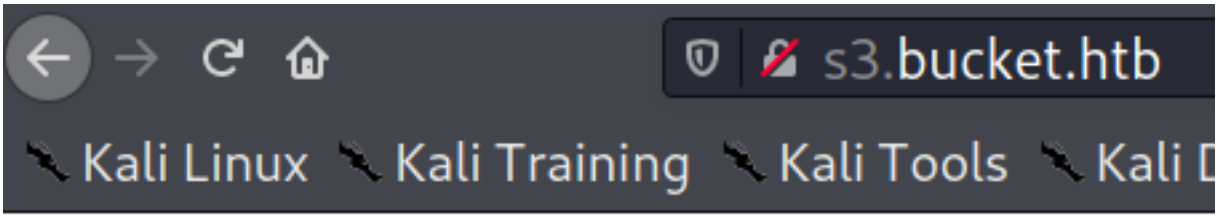
gobuster also yeilded no result

```
[ERROR] 2021/05/04 02:22:36 [!] Get "http://bucket.htb/gethelp.txt": context deadline exceeded (Clie
[ERROR] 2021/05/04 02:27:16 [!] Get "http://bucket.htb/Smart_Cards.txt": context deadline exceeded
[ERROR] 2021/05/04 02:28:59 [!] Get "http://bucket.htb/third.ph": context deadline exceeded (Client
[ERROR] 2021/05/04 02:31:08 [!] Get "http://bucket.htb/4932.php": context deadline exceeded (Client
cket.htb/2172639": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2021/05/04 02:31:14 [!] Get "http://bucket.htb/assistants_personnels": context deadline exce
[ERROR] 2021/05/04 02:31:14 [!] Get "http://bucket.htb/treiber": context deadline exceeded (Client.T
[ERROR] 2021/05/04 02:31:30 [!] Get "http://bucket.htb/040224.ph": context deadline exceeded (Client
[ERROR] 2021/05/04 02:37:33 [!] Get "http://bucket.htb/release11_8.html": context deadline exceeded
[ERROR] 2021/05/04 02:37:40 [!] Get "http://bucket.htb/_dl.txt": context deadline exceeded (Client.T
```

so going through the source code we see a new domain name which we have to add andd see where it lands us

```
<article>
<div class="coffee">
<img src="http://s3.bucket.htb/adserver/images/bug.jpg" alt="Bug" height="160" width="160">
</div>
```

here we can see s3.bucket.htb
so lets add it to the host file



{"status": "running"}

the page shows this but we can run the gobuster on it and we will see what output we get

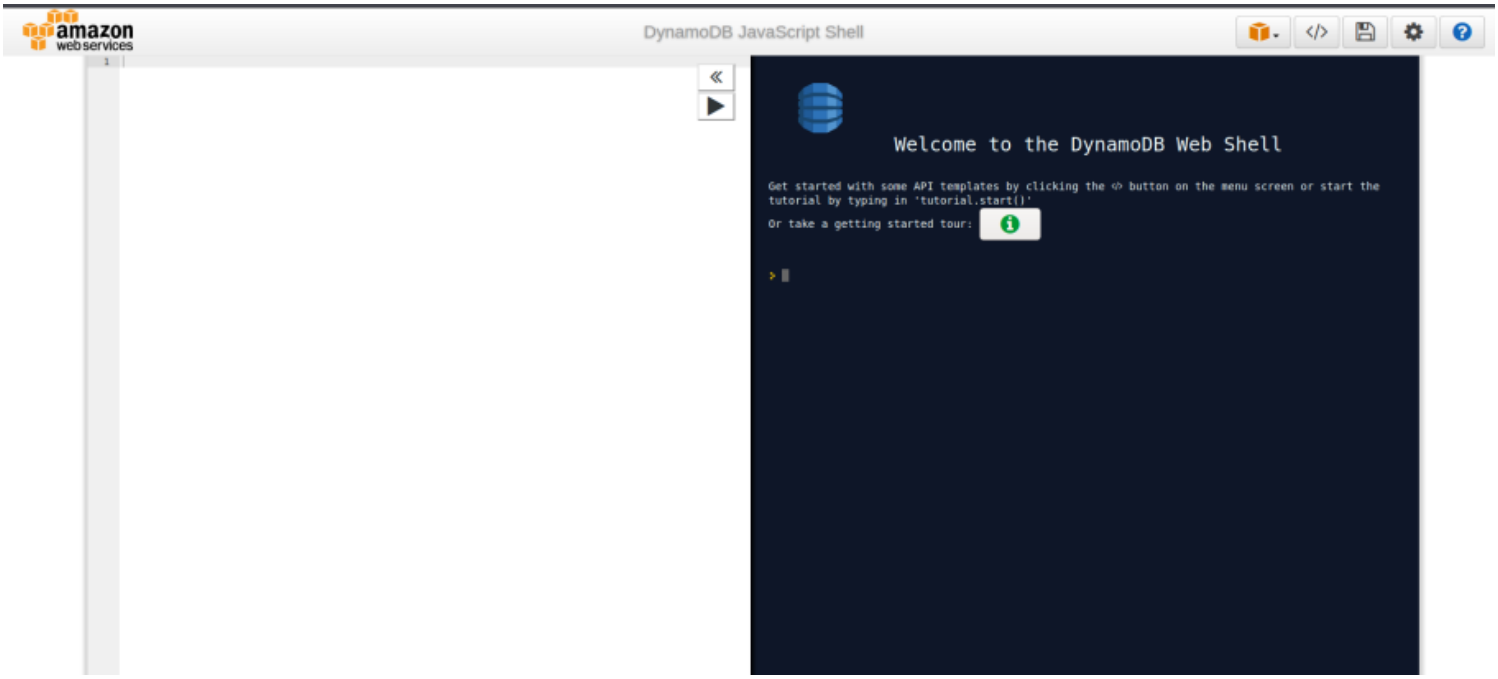
```
/health                 (Status: 200) [Size: 54]
/shell                  (Status: 200) [Size: 0]
/shell.txt              (Status: 500) [Size: 158]
/shell.php              (Status: 500) [Size: 158]
/shell.html             (Status: 500) [Size: 158]
/shell.ph               (Status: 500) [Size: 158]
/shellcode              (Status: 500) [Size: 158]
/shellcode.html         (Status: 500) [Size: 158]
/shellcode.ph           (Status: 500) [Size: 158]
/shellcode.txt          (Status: 500) [Size: 158]
/shellcode.php          (Status: 500) [Size: 158]
/shells                 (Status: 500) [Size: 158]
/shells.txt             (Status: 500) [Size: 158]
/shells.php             (Status: 500) [Size: 158]
/shells.html            (Status: 500) [Size: 158]
/shells.ph              (Status: 500) [Size: 158]
/shellscripts           (Status: 500) [Size: 158]
/shellscripts.txt       (Status: 500) [Size: 158]
/shellscripts.php       (Status: 500) [Size: 158]
/shellscripts.html      (Status: 500) [Size: 158]
/shellscripts.ph        (Status: 500) [Size: 158]
Progress: 88565 / 1102805 (8.03%)                ^C
[!] Keyboard interrupt detected, terminating.
```

so we have couple of directories and files lets see them one by one

```
▼ services:
    s3:         "running"
    dynamodb:   "running"
```

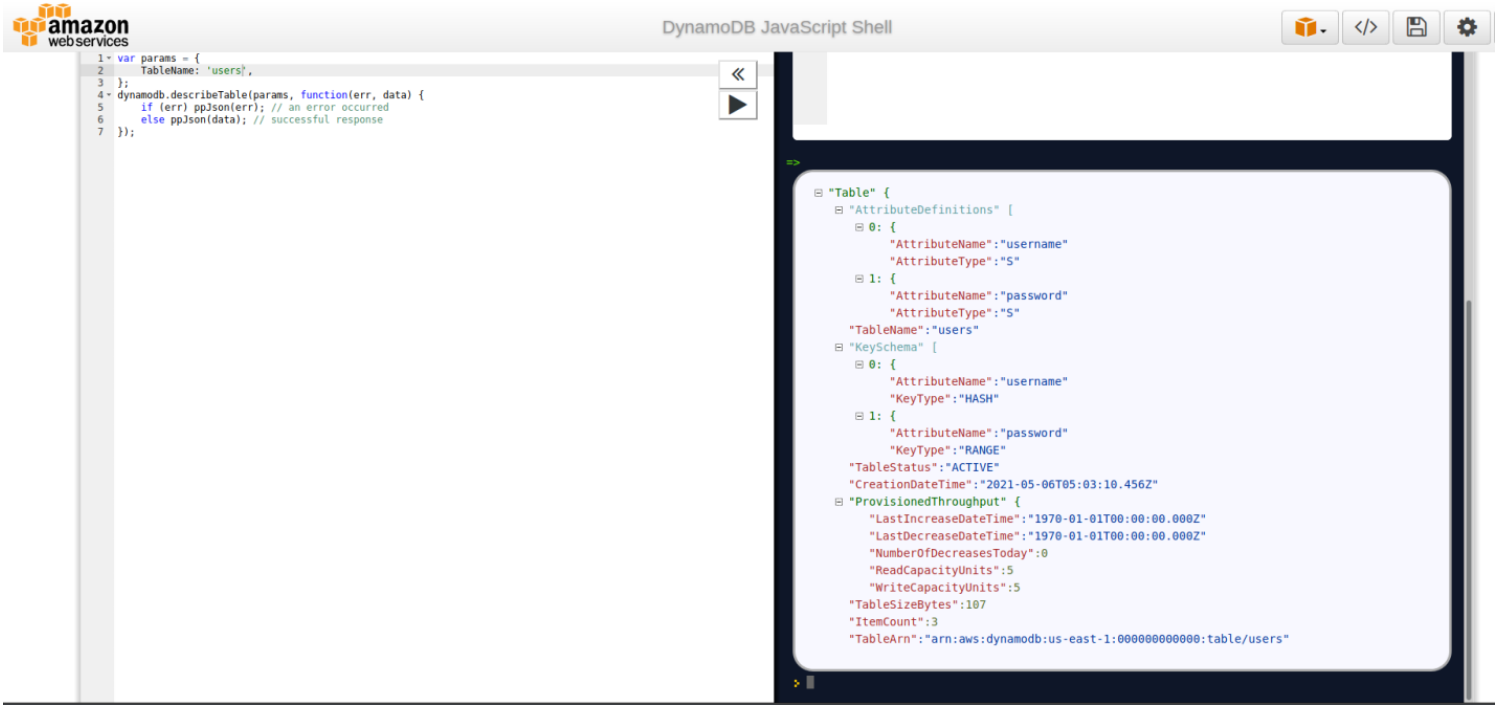
so we can see that dynamodb is running lets see other directories

going to /shell we found a page

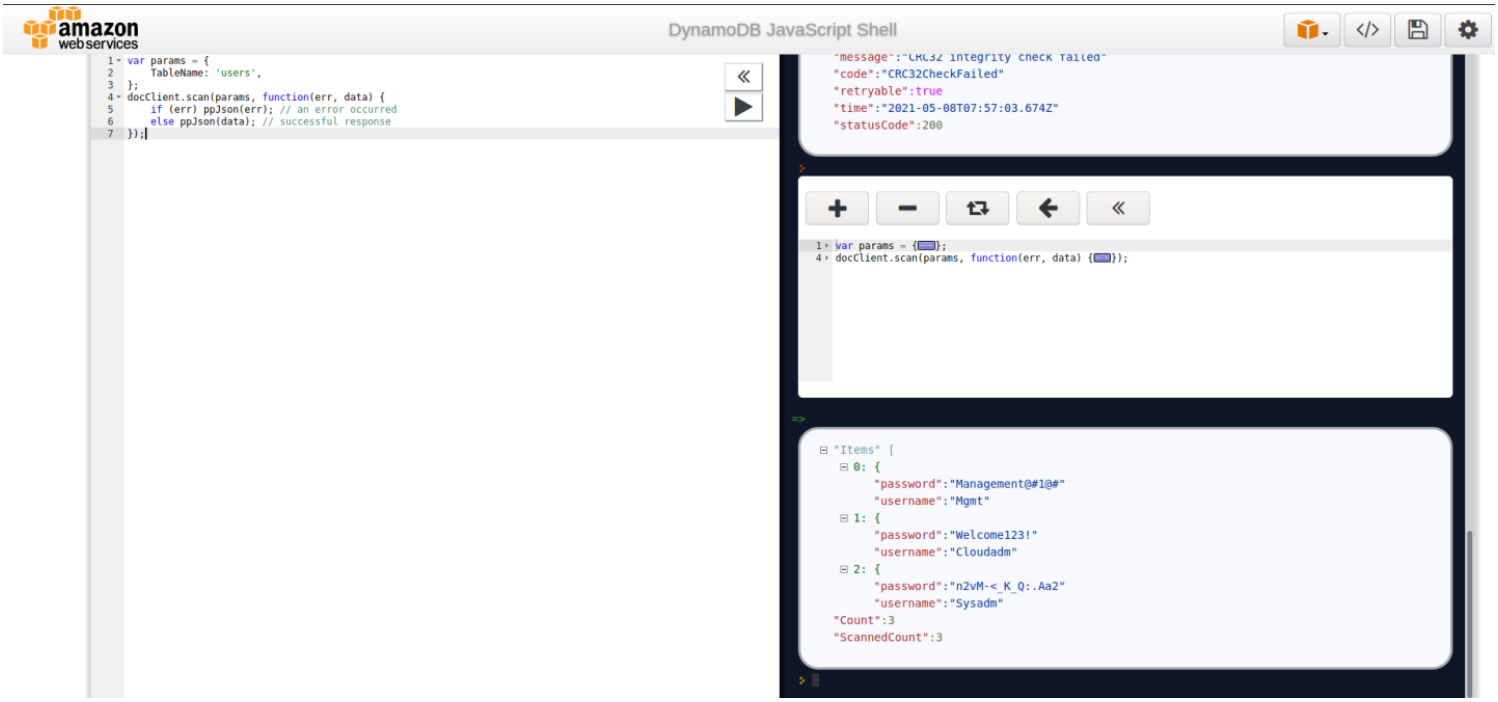


we see it is a webshell hosted on aws

after going through some tutorial and finding so much we saw a script to describe table and table name "users" which dumps some useful details



we saw table has attribute username and password now we have to scan to get the data from the table



it is non capy from dynamodb so credentials are

{Mgmt:Management@#1@#}{Cloudadm:Welcome123!}{Sysadm:n@vM-<_K_Q:.Aa2}

so now as we have credentils we have to see where we can use it to get some access