SteamCloud

```
└──# nmap -sCV -p 22,2380,8443,10250 -A 10.10.11.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 03:28 PDT
Nmap scan report for 10.10.11.133
Host is up (0.23s latency).

PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 fc:fb:90:ee:7c:73:a1:d4:bf:87:f8:71:e8:44:c6:3c (RSA)
|   256 46:83:2b:1b:01:db:71:64:6a:3e:27:cb:53:6f:81:a1 (ECDSA)
|_  256 1d:8d:d3:41:f3:ff:a4:37:e8:ac:78:08:89:c2:e3:c5 (ED25519)
2380/tcp  open  ssl/etcd-server?
| ssl-cert: Subject: commonName=steamcloud
| Subject Alternative Name: DNS:localhost, DNS:steamcloud, IP Address:10.10.11.133, IP
Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1
| Not valid before: 2024-06-03T10:26:30
|_Not valid after:  2025-06-03T10:26:31
| tls-alpn:
|_  h2
|_ssl-date: TLS randomness does not represent time
8443/tcp  open  ssl/https-alt
| tls-alpn:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=minikube/organizationName=system:masters
| Subject Alternative Name: DNS:minikubeCA, DNS:control-plane.minikube.internal,
DNS:kubernetes.default.svc.cluster.local, DNS:kubernetes.default.svc,
DNS:kubernetes.default, DNS:kubernetes, DNS:localhost, IP Address:10.10.11.133, IP
Address:10.96.0.1, IP Address:127.0.0.1, IP Address:10.0.0.1
| Not valid before: 2024-06-02T10:26:29
|_Not valid after:  2027-06-03T10:26:29
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 403 Forbidden
|     Audit-Id: 6ec7fd63-e0dc-4be9-97bd-639da822b129
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
```

```
|     X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
|     Date: Mon, 03 Jun 2024 10:29:11 GMT
|     Content-Length: 212
|     {"kind":"Status","apiVersion":"v1","metadata":
{},"status":"Failure","message":"forbidden: User "system:anonymous" cannot get path
"/nice ports,/Trinity.txt.bak"","reason":"Forbidden","details":{},"code":403}
|   GetRequest:
|     HTTP/1.0 403 Forbidden
|     Audit-Id: 7dbf7e9d-6ae1-45ab-9118-dd02ba34b609
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
|     X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
|     Date: Mon, 03 Jun 2024 10:29:09 GMT
|     Content-Length: 185
|     {"kind":"Status","apiVersion":"v1","metadata":
{},"status":"Failure","message":"forbidden: User "system:anonymous" cannot get path
"/"","reason":"Forbidden","details":{},"code":403}
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Audit-Id: ecde9564-176e-4641-ba60-fa00a55202d2
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 7ee25ed4-1110-4366-8b72-26d0d4a5b3c2
|     X-Kubernetes-Pf-Prioritylevel-Uid: 04d99ffe-e3c6-42e1-b353-c90e308ba10c
|     Date: Mon, 03 Jun 2024 10:29:10 GMT
|     Content-Length: 189
|_    {"kind":"Status","apiVersion":"v1","metadata":
{},"status":"Failure","message":"forbidden: User "system:anonymous" cannot options
path "/"","reason":"Forbidden","details":{},"code":403}
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (application/json).
10250/tcp open  ssl/http        Golang net/http server (Go-IPFS json-rpc or InfluxDB
API)
| tls-alpn:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=steamcloud@1717410393
| Subject Alternative Name: DNS:steamcloud
| Not valid before: 2024-06-03T09:26:33
```

|_Not valid after: 2025-06-03T09:26:33
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
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-Port8443-TCP:V=7.94SVN%T=SSL%I=7%D=6/3%Time=665D9AF5%P=aarch64-unknown-
SF:linux-gnu%r(GetRequest,22F,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\
SF:x207dbf7e9d-6ae1-45ab-9118-dd02ba34b609\r\nCache-Control:\x20no-cache,\
SF:x20private\r\nContent-Type:\x20application/json\r\nX-Content-Type-Optio
SF:ns:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366
SF:-8b72-26d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3
SF:c6-42e1-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:2
SF:9:09\x20GMT\r\nContent-Length:\x20185\r\n\r\n{\"kind\":\"Status\",\"api
SF:Version\":\"v1\",\"metadata\":{},\"status\":\"Failure\",\"message\":\"f
SF:orbidden:\x20User\x20\\\"system:anonymous\\\"\x20cannot\x20get\x20path\
SF:x20\\\"/\\\"\",\"reason\":\"Forbidden\",\"details\":{},\"code\":403}\n"
SF:)%r(HTTPOptions,233,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\x20ecde
SF:9564-176e-4641-ba60-fa00a55202d2\r\nCache-Control:\x20no-cache,\x20priv
SF:ate\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20
SF:nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366-8b72-2
SF:6d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3c6-42e1
SF:-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:29:10\x2
SF:0GMT\r\nContent-Length:\x20189\r\n\r\n{\"kind\":\"Status\",\"apiVersion
SF:\":\"v1\",\"metadata\":{},\"status\":\"Failure\",\"message\":\"forbidde
SF:n:\x20User\x20\\\"system:anonymous\\\"\x20cannot\x20options\x20path\x20
SF:\\\"/\\\"\",\"reason\":\"Forbidden\",\"details\":{},\"code\":403}\n")%r
SF:(FourOhFourRequest,24A,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\x206
SF:ec7fd63-e0dc-4be9-97bd-639da822b129\r\nCache-Control:\x20no-cache,\x20p
SF:rivate\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\
SF:x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x207ee25ed4-1110-4366-8b7
SF:2-26d0d4a5b3c2\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x2004d99ffe-e3c6-4
SF:2e1-b353-c90e308ba10c\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2010:29:11
SF:\x20GMT\r\nContent-Length:\x20212\r\n\r\n{\"kind\":\"Status\",\"apiVers
SF:ion\":\"v1\",\"metadata\":{},\"status\":\"Failure\",\"message\":\"forbi
SF:dden:\x20User\x20\\\"system:anonymous\\\"\x20cannot\x20get\x20path\x20\
SF:\\"/nice\x20ports,/Trinity\.txt\.bak\\\"\",\"reason\":\"Forbidden\",\"d
SF:etails\":{},\"code\":403}\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).

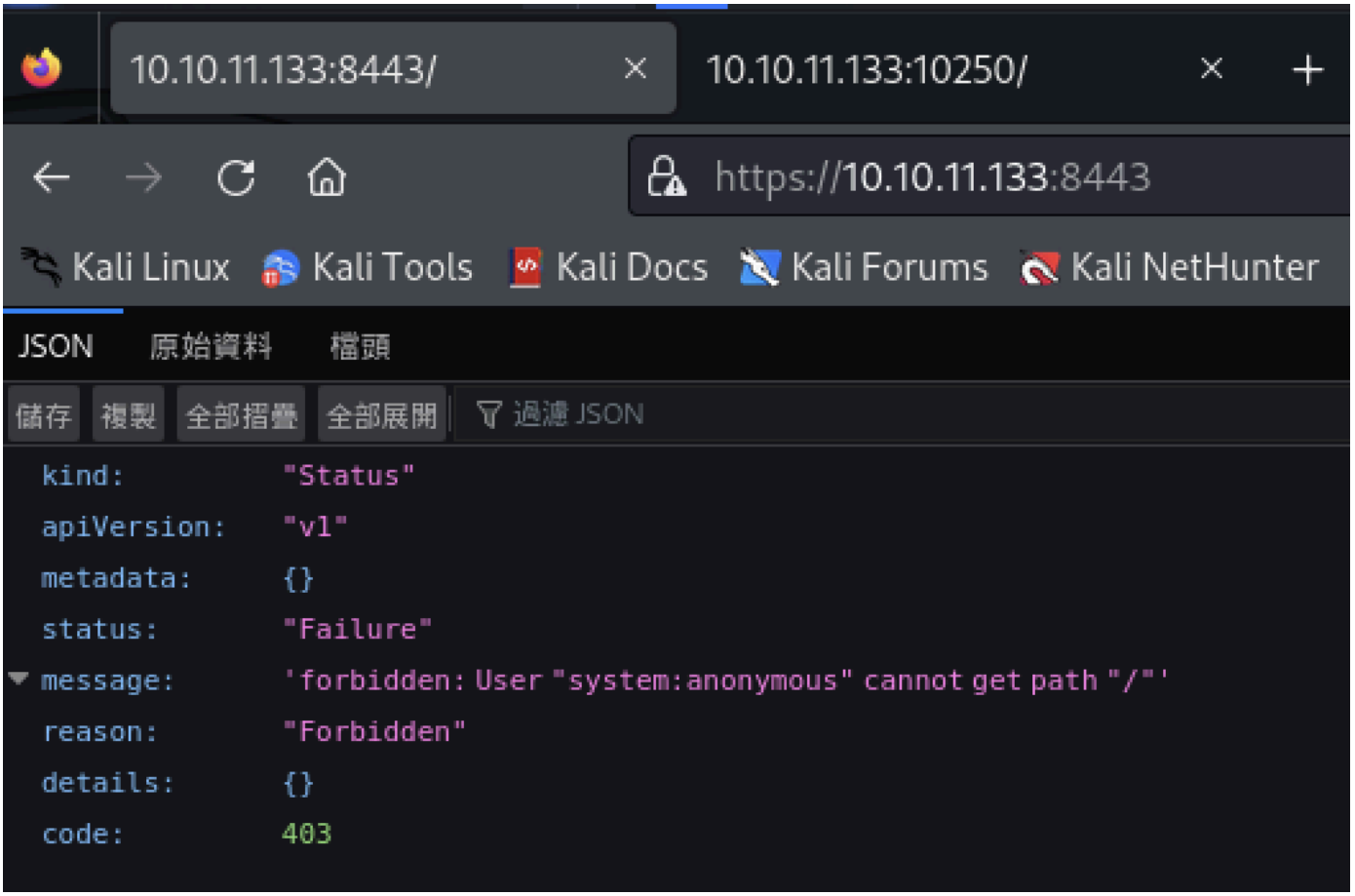
```
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   282.12 ms 10.10.14.1
2   282.37 ms 10.10.11.133

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.91 seconds
```

---

web8443



8443Port憑證(端口掃描的)

```
ssl-cert: Subject:
commonName=minikube/organizationName=system:masters

Subject Alternative Name:
DNS:minikubeCA,
DNS:control-plane.minikube.internal,
DNS:kubernetes.default.svc.cluster.local,
DNS:kubernetes.default.svc,
DNS:kubernetes.default,
```

```
DNS:kubernetes,
DNS:localhost,
IP Address:10.10.11.133,
IP Address:10.96.0.1,
IP Address:127.0.0.1,
IP Address:10.0.0.1
```

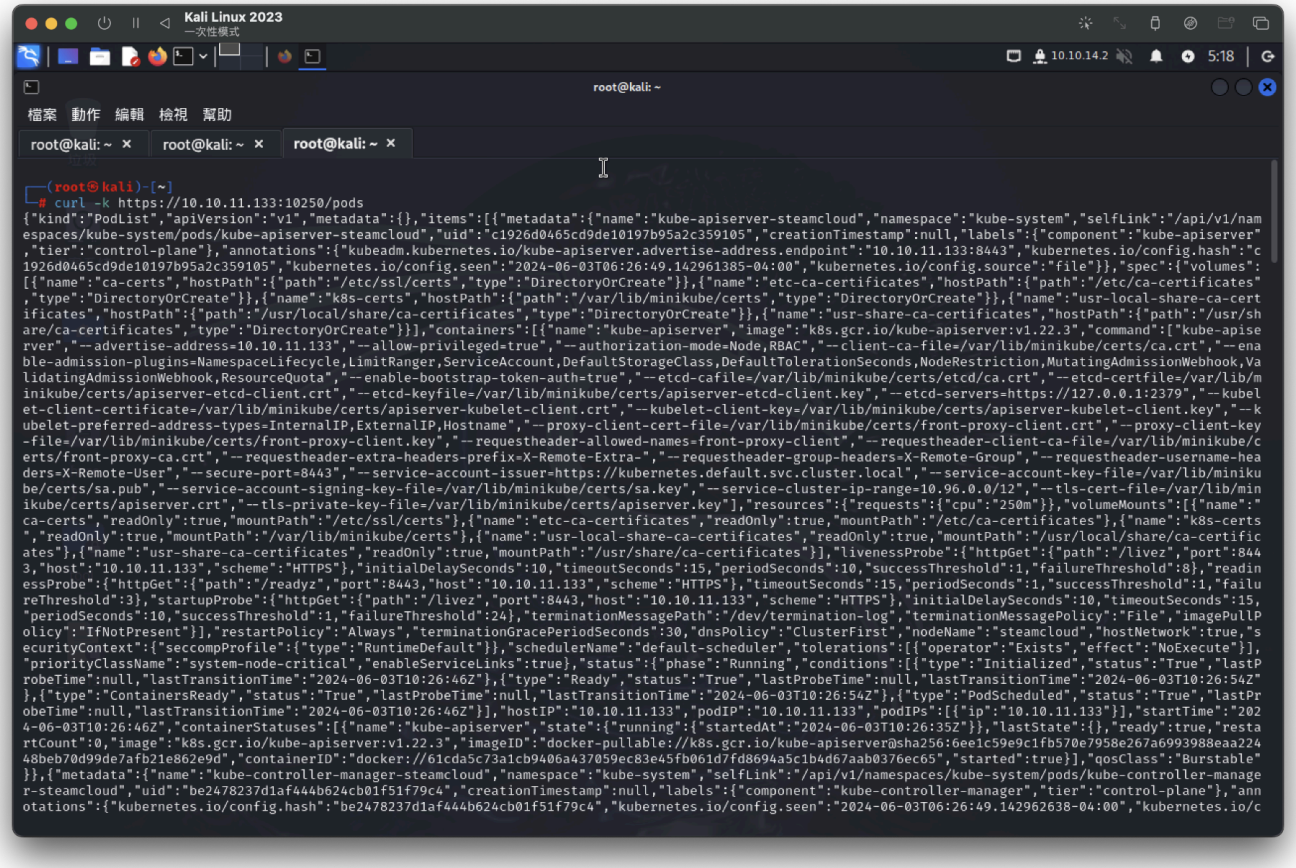
似乎跟kubernetes有關

參考原廠文件：https://kubernetes.io/docs/concepts/overview/

滲透文件：https://cloud.hacktricks.xyz/pentesting-cloud/kubernetes-security/pentesting-kubernetes-services

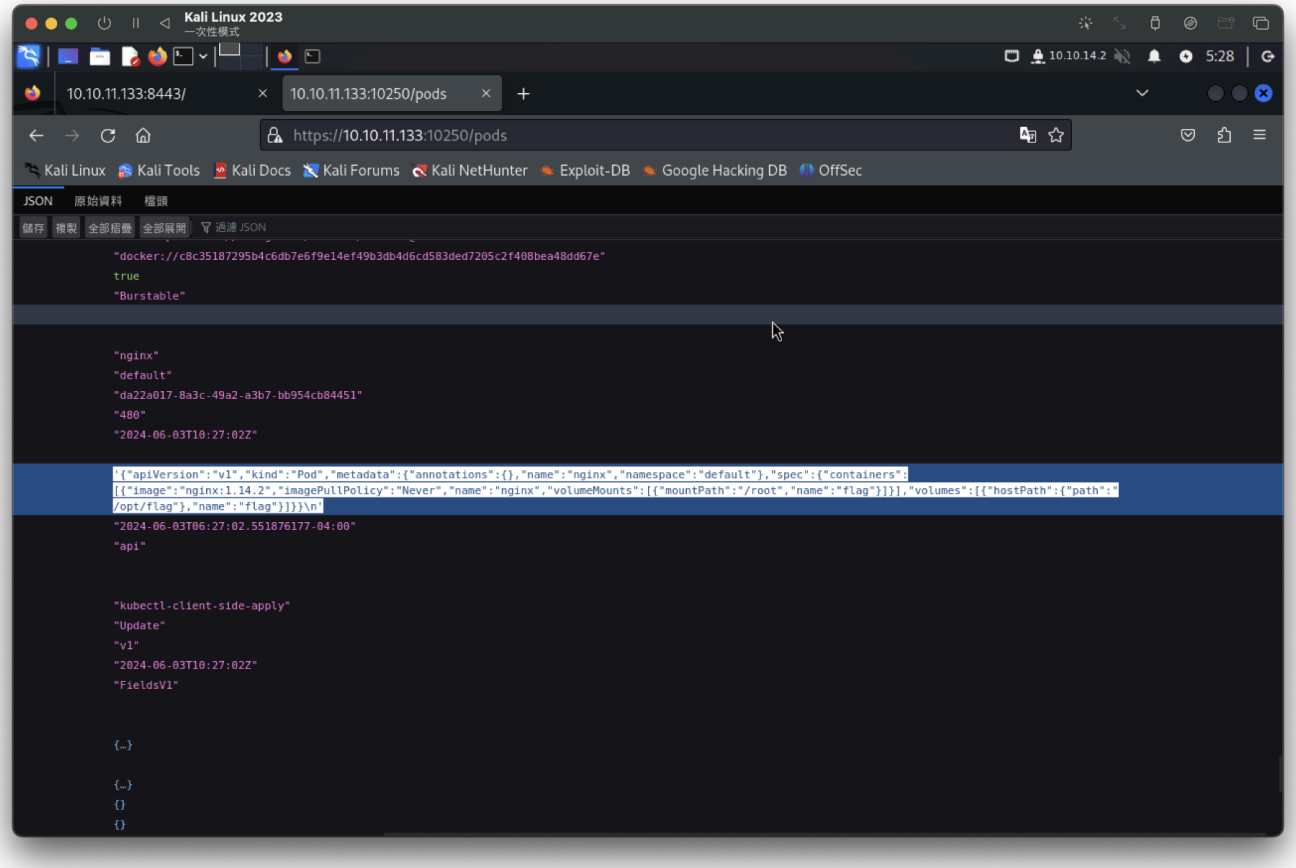
工具：https://github.com/cyberark/kubeletctl

手動測試



太亂了，工具也要弄一堆東西放棄，

用web手動查找，找到有關root字眼




```
name : nginx
```

但需要工具才能反彈。。。

工具弄不好