Network Security Audit

A1Target Metasploitable2

Submitted By

Uddeshya Sinha

IN 618 Security

Feb-June 2018

Lecturer

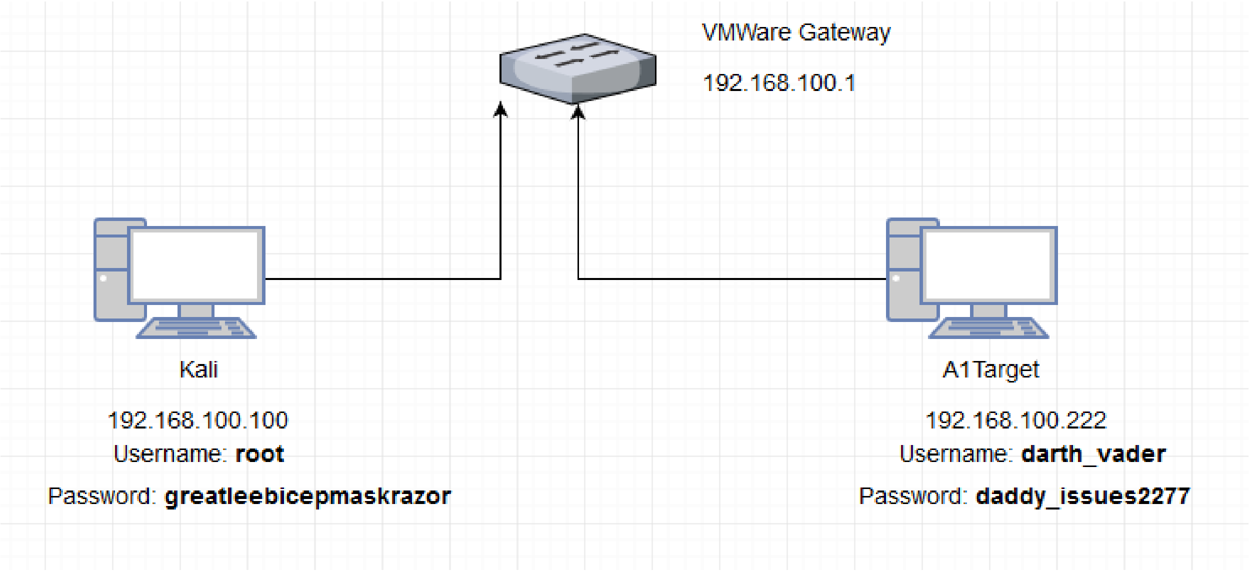
Dr. Thomas Laurenson

Date: **Tuesday 10th April**

Executive Summary

The major objective of the security audit is to find and extract valuable information from a remote Metasploitable2 server. The extraction of information was possible because of several vulnerabilities found on the open ports in the server. Since, there is no firewall implemented on the Metasploitable2 server, all the open ports along with the services running on them is visible to the attacker. Vulnerabilities on port 21, 22 and the irc ports- 6667, 6697, and 8067 have been found. Exploitation of any of the irc ports provides the remote access to the Metasploitable2 server but not as a super user. However, gaining access as a super user wasn't difficult as the password for darth_vader was sitting in the boba_fett folder in the home directory. This makes the vulnerability to be of high severity. One of the other two vulnerabilities is of high severity (ftp) as it gives remote access to the web configuration files and the last one is of medium severity (ssh). For strengthening the security of the remote server, a strong firewall must be in place along with updated software services running on it. Finally, the password for a super user such as darth_vader should not be saved as plaintext.

1) HOST DISCOVERY


VMWare Gateway
192.168.100.1
Kali
192.168.100.100
Username: **root**
Password: **greatleebicepmaskrazor**
A1Target
192.168.100.222
Username: **darth_vader**
Password: **daddy_issues2277**

First of all, the Kali VM's IP address was found to be **192.16.100.100** by running the command "ifconfig". We know that the target machine is in the same network. So, by using the nmap command "nmap –sn 192.168.100.*" ("Host Discovery | Nmap Network Scanning", n.d.), the target's machine IP address and the MAC address if discovered and documented below:

- Target hostname: A1Target
- Target IP address: 192.168.100.222
- Target MAC address: 00:50:56:86:4C:4F
- Operating System (reported by nmap): Linux 3.X/4.X

  Running (reported by nmap): Linux 3.10 – 4.8
- Actual Operating System Version: Ubuntu 14.04.1 LTS

  Actual Linux Kernel version: Linux 3.13.0-32-generic x86_64
- Username: darth_vader

- Password: daddy_issues2277

2) Information Gathering

For determining the open ports and the associated services running on them, nmap's command "nmap –sV -p- 192.168.100.222" (Duc, 2015) was used. The result shows all the open ports and the services running on them. A total of 13 open ports were found open and the rest 65,522 ports were closed as listed below:

PORT	STATE	SERVICE	VERSION
21/tcp	Open	ftp	ProFTPD 1.3.5
22/tcp	Open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10
80/tcp	Open	http	Apache httpd 2.4.7
111/tcp	Open	rpcbind	2-4 (RPC #100000)
139/tcp	Open	netbios-ssn	Samba smbd 3.X - 4.X
445/tcp	Open	netbios-ssn	Samba smbd 3.X - 4.X
3306/tcp	Open	mysql	MySQL (unauthorized)
6667/tcp	Open	irc	UnrealIRCd
6697/tcp	Open	irc	UnrealIRCd
8067/tcp	Open	irc	UnrealIRCd
8080/tcp	Open	http	Jetty 8.1.7.v20120910

8181/tcp	Open	http	WEBrick httpd 1.3.1 (Ruby 2.3.6 (2017-12-14))
52319/tcp	Open	status	1 (RPC #100024)

3) Vulnerability Identification and Exploitation

Vulnerabilities were found on 5 ports (out of which 3 runs the same service).

1) *Vulnerability on port 6667, 6697 and 8067 (irc)*

The most crucial exploit of the target server as it resulted in accessing the target remotely as a normal user named “boba-fett”. Under the folder of “boba-fett”, there is a text file named “darth_vaders_password.txt” containing the password for the super-user “darth_vader” as plaintext.

Vulnerability Summary:

- Protocol: **Internet Relay Services** (IRC)
- Port Number: **6667, 6697, 8067**
- Software Name: **UnrealIRCd**
- Software Version: **3.2.8.1**

Exploit Summary: ("CVE-2010-2075 UnrealIRCD 3.2.8.1 Backdoor Command Execution | Rapid7", n.d.)

- Discovered: **search exploit database for “search unrealircd”**
- Exploit Tool: **Metasploit Framework**
- Exploit Name: **UnrealIRCD 3.2.8.1 Backdoor Command Execution**
- Payload: **cmd/unix/reverse**
- URL: https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor
- Source Code: **https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/irc/unreal_ircd_3281_backdoor.rb**
- Exploit Result: **Successful** (remote terminal as a normal user)
- Severity: **High**
- CVE Number: **CVE-2010-2075**
- Module: `exploit/unix/irc/unreal_ircd_3281_backdoor`
- Description: **This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010**.

2) *Vulnerability on port 21 (ftp)*

This vulnerability gives us access to the remote server as a user named “www.data”. Since, this user has the ownership to configure web files on Apache2 server, this exploit could be very dangerous for the remote server as the important web files could get exposed to the attacker.

Vulnerability Summary:

- Protocol: **File Transfer Protocol** (FTP)
- Port Number: **21**
- Software Name: **ProFTPD**
- Software Version: **1.3.5**

Exploit Summary: ("CVE-2015-3306 ProFTPD 1.3.5 Mod_Copy Command Execution | Rapid7", n.d.)

- Discovered: **search exploit database for “search proftpd”**
- Exploit Tool: **Metasploit Framework**
- Exploit Name: **ProFTPD 1.3.5 Mod_Copy Command Execution**
- Payload: **cmd/unix/bind_perl**
- URL: https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec
- Source Code: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/proftpd_modcopy_exec.rb
- Exploit Result: **Successful** (remote terminal as user “www.data”)
- Severity: **High**
- CVE Number: CVE-2015-3306
- Module: `exploit/unix/ftp/proftpd_modcopy_exec`
- Description: **This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination**.

3) *Vulnerability on port 22 (ssh)*

This vulnerability could be of great importance only if the attacker gets hold of a Username and a Password file of common passwords. These files could be used to brute-force against different username-password combination. ("Scanner SSH Auxiliary Modules", n.d.) All the passwords for the users are present in the “rockyou.txt” file. The home directory of the target machine has all the usernames and putting these usernames in a text file would give us our Username file to brute force along with the rockyou.txt file.

Vulnerability Summary:

- Protocol: **Secure Shell** (SSH)
- Port Number: **22**
- Software Name: **OpenSSH**

- Software Version: **6.6.1**

Exploit Summary: ("CVE-1999-0502 SSH Login Check Scanner | Rapid7", n.d.)

- Discovered: **search exploit database for "search ssh"**
- Exploit Tool: **Metasploit Framework**
- Exploit Name: **SSH Login Check Scanner**
- URL: **https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_login**
- Source Code: **https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssh/ssh_login.rb**
- Exploit Result: **Successful** (remote terminal as root user)
- Severity: **Medium**
- CVE Number: CVE-1999-0502
- Module: **use auxiliary/scanner/ssh/ssh_login**
- Description: **This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.**

4) Information Extraction

All the information needed by the Rebel Alliance in order to destroy "death-star" is provided below. The table below contains information about each person involved in the "death-star" along with their passwords.

Summary:

Tool: Hashcat 4.1.0

- File: /etc/shadow
- Hashing Algorithm: Message Digest 5 (MD5)
- Salting Method: md5(salt + hash)
- Hashcat Algorithm Mode: Mode 500 (md5crypt)

Logged in as one of the super user. Access the shadow file which has the salts and hashes for each user and also information about the hashing algorithm. "$1" which means the hashing algorithm is MD5. A new text file called "assignment.txt" was created in the hashcat folder and the contents of the shadow file was added to it. Make sure that the file "rockyou.txt" is present in the hashcat folder. 15 passwords for 15 users was extracted using hashcat in Windows Powershell. The password for the user "vagrant" was not extracted.

Hashcat command for password retrieval: **hashcat64.exe -m 500 assignment.txt rockyou.txt**

USERNAME	SALT	HASH	Plaintext-Password
storm_trooper_1	mhzU7fKc	3kI1bYA7VcD28TvsZB/rY/	theDARKside
storm_trooper_2	Oq2zvoKD	nf7zaPAFuPfT0LNRZrv91/	stillup2nogood
storm_trooper_3	Ury0Ax4Z	a5XSPA6ID1BA/0msCmN8/0	darksidethugs
storm_trooper_4	GDYbz3x8	5oYuMe5krxnX//wNeR7P11	supertrooper
storm_trooper_5	flxe38hz	VOaLPAoE6eO7JeWFMsBZS.	kittenswithmittens
imperial_guards	K6jM.Fyf	YOlctYfbkT.BGx913.SDb/	darkside2700
boba_fett	vT1OA4dm	oNGwR/9tffr3eJv30WpuS.	bountyhunter1976
captain_needa	r/imXmvK	tj.uveUEE/tnD.eZcNYIy.	darksidegod@hotmail.com
general_veers	tsWMwd/T	VY1DCNtWBSNSBXlp9GaLI0	darkside131
admiral_piett	iWH9/gx.	njNg/iimHFO6ZAxaZrfW81	DarkSideForever0
admiral_ozzel	/l/zGQCr	RVoUXL8QDGTgxJ7FrZamf/	theadmiral
death_star_admin	C8hQ8YVy	qLlODYV.XRA8FeJmV6Q5u/	deathstar313
emperor_palpatine	sF67XzYD	kTPzQAS4bhFnKUrxvGY.x0	darkside!
darth_vader	dqkERFiQ	oMihN1usY.gnbemCa48Pk1	daddy_issues2277
darth_sidious	udZXIBn5	7v57gK8MQn6PPfVDbrYg40	darksideismine

Death-star plans leaked!

A total of 8 files were found on the target machine which contains sensitive information about the death-star project. The deathstar files were found by using the find command with the grep command with the keywords “deathstar” and “death-star”

- 5 of the files – **deathstar-crafts.PNG**

  deathstar-cross-section.PNG

  deathstar-operations.PNG

  deathstar-summary.PNG

  deathstar-technical-specs-diagram.PNG

  were found in the location **/home/death_star_admin.**

- 1 of the files – **deathstarinfographic.PNG**

  was found in the location **/opt/proftpd/share/locale**

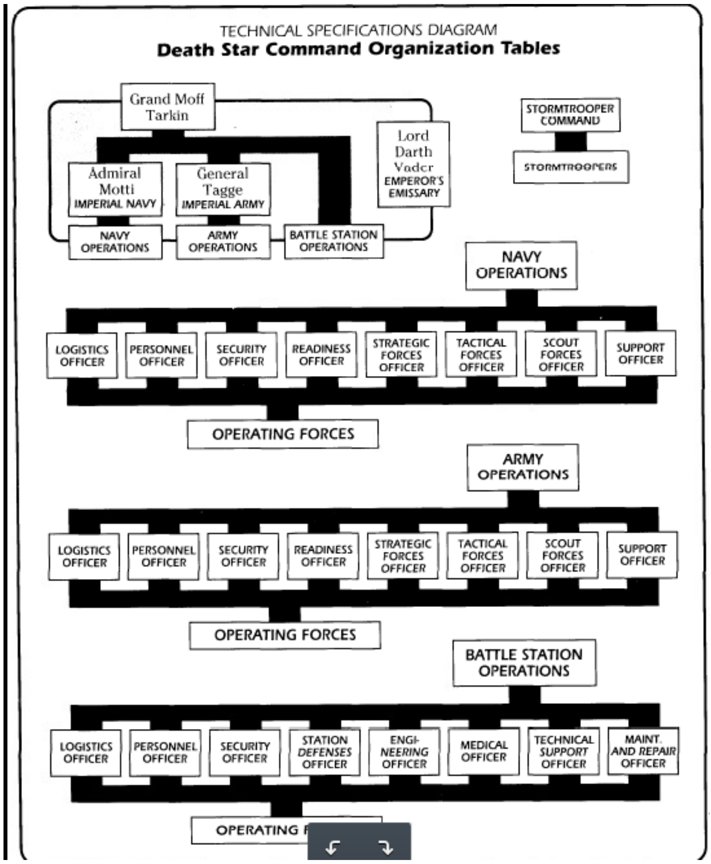
- 1 of the files –**death-star- our only weakness.PNG**

  was found in the location **/home/darth_sidious**

- 1 of the files – **i-love-my-death-star.jpg**

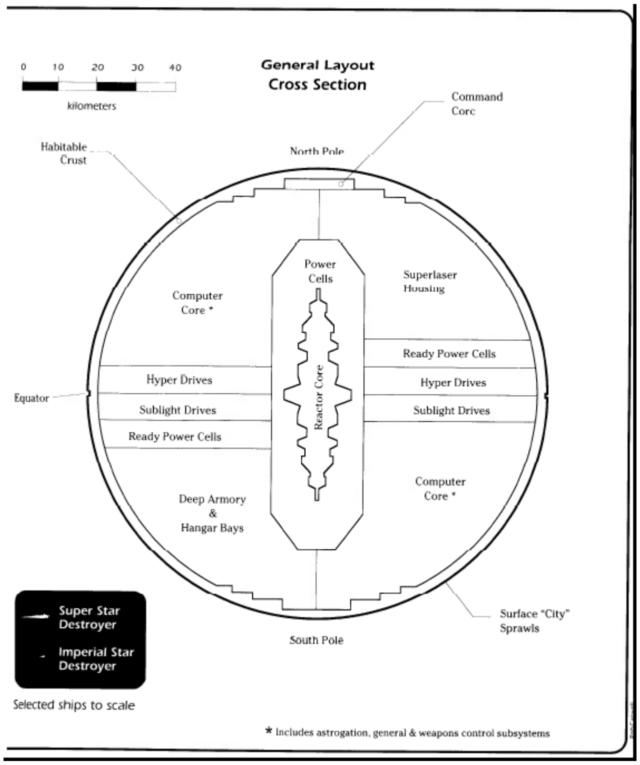
  Was found in the location **/home/darth_vader**

  Below are the screenshots of the death-star plans:



TECHNICAL SPECIFICATIONS DIAGRAM

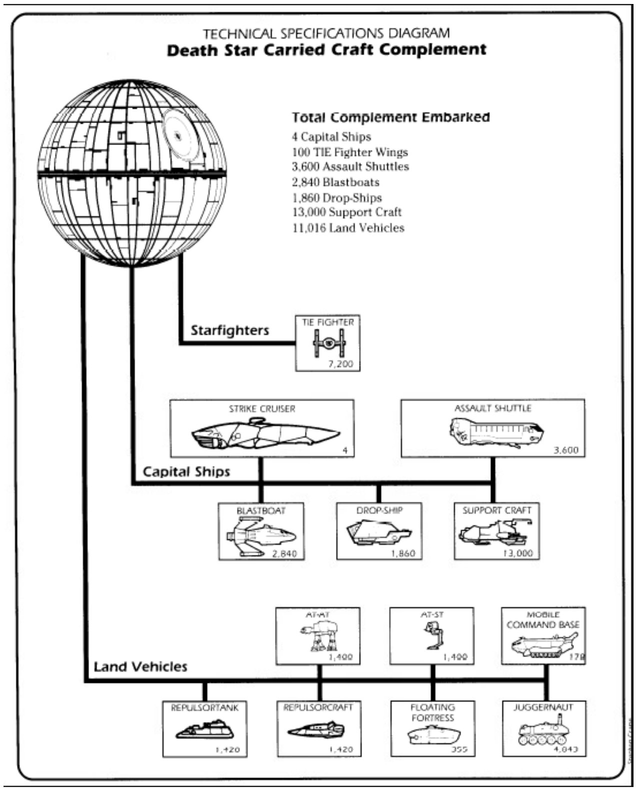
Death Star Command Organization Tables



General Layout
Cross Section

Selected ships to scale

* Includes astrogation, general & weapons control subsystems

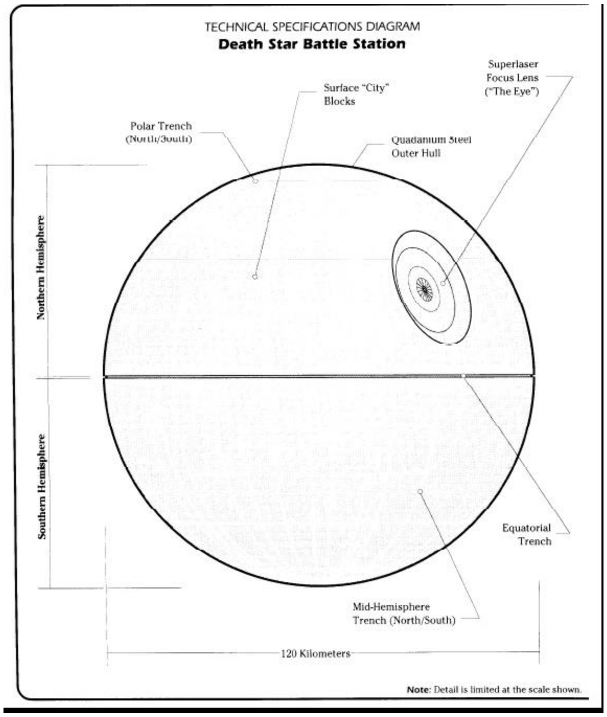


TECHNICAL SPECIFICATIONS DIAGRAM

Death Star Carried Craft Complement

Total Complement Embarked

4 Capital Ships
100 TIE Fighter Wings
3,600 Assault Shuttles
2,840 Blastboats
1,860 Drop-Ships
13,000 Support Craft
11,016 Land Vehicles



TECHNICAL SPECIFICATIONS DIAGRAM

Death Star Battle Station

Note: Detail is limited at the scale shown.

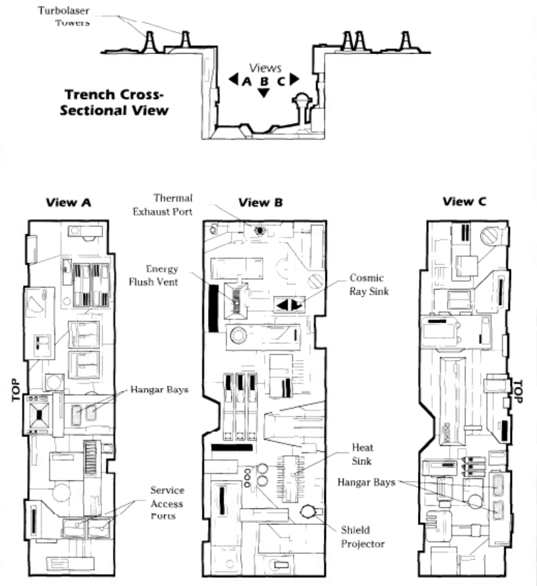
Death Star
Battle Station

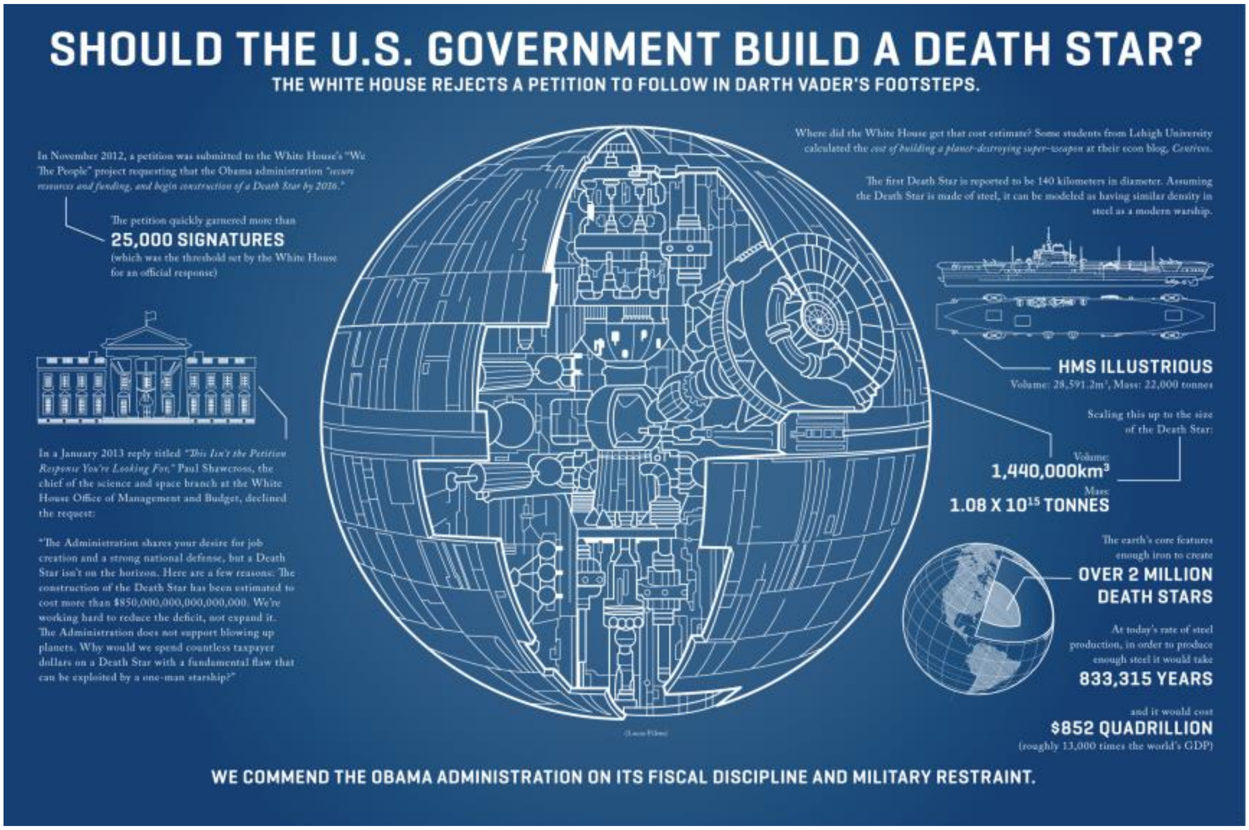
Craft: Custom Deep Space Battle Station
Type: Deep space mobile battle station
Scale: Death Star
Length: 120 kilometers (diameter)
Skill: Battle station piloting: Death Star
Crew: 265,675, gunners: 57,276, skeleton 56,914/+15
Crew Skill: Astrogation 5D+1, battle station piloting 6D, capital ship gunnery 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.

CITY SPRAWLS AND TRENCHES DIAGRAM
Typical Surface Trench





SHOULD THE U.S. GOVERNMENT BUILD A DEATH STAR?

THE WHITE HOUSE REJECTS A PETITION TO FOLLOW IN DARTH VADER'S FOOTSTEPS.

In November 2012, a petition was submitted to the White House's "We The People" project requesting that the Obama administration *"secure resources and funding, and begin construction of a Death Star by 2016."*

The petition quickly garnered more than

25,000 SIGNATURES

(which was the threshold set by the White House for an official response)

In a January 2013 reply titled *"This Isn't the Petition Response You're Looking For,"* Paul Shawcross, the chief of the science and space branch at the White House Office of Management and Budget, declined the request:

"The Administration shares your desire for job creation and a strong national defense, but a Death Star isn't on the horizon. Here are a few reasons: The construction of the Death Star has been estimated to cost more than $850,000,000,000,000,000. We're working hard to reduce the deficit, not expand it. The Administration does not support blowing up planets. Why would we spend countless taxpayer dollars on a Death Star with a fundamental flaw that can be exploited by a one-man starship?"

Where did the White House get that cost estimate? Some students from Lehigh University calculated the *cost of building a planet-destroying super-weapon* at their econ blog, *Centives.*

The first Death Star is reported to be 140 kilometers in diameter. Assuming the Death Star is made of steel, it can be modeled as having similar density in steel as a modern warship.

HMS ILLUSTRIOUS

Volume: $28,591.2\text{m}^3$, Mass: 22,000 tonnes

Scaling this up to the size of the Death Star:

Volume:
$1,440,000\text{km}^3$

Mass:
1.08×10^{15} TONNES

The earth's core features enough iron to create

OVER 2 MILLION DEATH STARS

At today's rate of steel production, in order to produce enough steel it would take

833,315 YEARS

and it would cost

$852 QUADRILLION

(roughly 13,000 times the world's GDP)

(Lucas Films)

WE COMMEND THE OBAMA ADMINISTRATION ON ITS FISCAL DISCIPLINE AND MILITARY RESTRAINT.

5) Security Recommendations

a) **Outdated OS**

The metasploitable2 server runs an older version of Ubuntu Linux i.e. 14.04. There are many security problems with this old version. Out-of-bounds write vulnerability (CVE-2017-0750), denial-of-service code execution (CVE-2017-0861), netlink wireless configuration interface vulnerability (CVE-2017-12153) to name a few.

Recommendation: These problems could be mitigated if the OS is upgraded to Ubuntu 17.10 which is the latest version.

b) **Outdated Software Services**

The services running on the open ports are all outdated, which is one of the major reason for the target machine being susceptible to remote code execution attacks.

Port	Metasploitable2 Outdated Version	New Stable Release
21	Proftpd 1.3.5	Proftpd 1.3.6
22	OpenSSH 6.6.1	OpenSSH 7.6
80	Apache Httpd 2.4	Apache Httpd 2.4.33
6667,6697,8067	IRC 3.2.8.1	IRC 3.7
8080	Jetty 8.1.7	Jetty 9.4.8
8181	WebRick Httpd 1.3.1	WebRick Httpd 1.3.9

Recommendation: The old version of Proftp could be exploited to upload or download files from the remote server by the attacker and hence it should be updated to the latest version.

There should only be a single port for a single service. Redundant services such as IRC running on three different ports should be avoided. Database service such as MySQL running is redundant as well.

c) **Firewall**

The open ports and the services running on them is visible to an attacker because the Metasploitable2 server doesn't have any firewall implemented to monitor the incoming/outgoing traffic.

Recommendation: There should be a firewall on the remote server so that the attacker could not figure out the vulnerabilities present on the server.

d) **User Passwords and the Hashing Algorithm**

Even though the user passwords are stored securely in the shadow file (which could only be accessed by a super user), password extraction using hashcat is possible since the passwords are very common. Another problem is that one of the super user's (darth_vader) password is stored in plaintext in a file which could even be accessed by other users with a lower privilege level. Also, the hashing algorithm used for hashing the passwords is MD5, which is found to have serious security consequences (especially brute-force attacks)

Recommendation: The users should never store their passwords in plaintext. A better hashing algorithm than MD5 should be used such as SHA256 or SHA512. The passwords should be stronger as they should contain a mixture of alphabets, numbers and special characters. A necessary password rule and a minimum password length would be suited for this job. The administrator of the server should encourage the users to change their passwords frequently.

6) Conclusion

In conclusion, since there are so many vulnerabilities resulting from outdated softwares, the softwares must always be up-to-date. A firewall with a strong policy should be in place to monitor incoming/outgoing packets. Strong passwords must always be used by all the legitimate users and they should be changed frequently as well. The security audit reflects the three major vulnerabilities which must be tackled at once. The Users should change their passwords immediately to avoid any security breaches. The server should be tested again and again on regular intervals to find any existing loopholes in the server.

7) References

Host Discovery | Nmap Network Scanning. (N.A.). Nmap.org. Retrieved 10 April 2018, from https://nmap.org/book/man-host-discovery.html

Duc, H. (2015). *Nmap - Gathering Additional Host Information - Pentestmag*. *Pentestmag*. Retrieved 10 April 2018, from https://pentestmag.com/nmap-gathering-additional-host-information/

CVE-1999-0502 SSH Login Check Scanner | Rapid7. *Rapid7.com*. Retrieved 10 April 2018, from https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_login

Scanner SSH Auxiliary Modules. *Offensive-security.com*. Retrieved 10 April 2018, from https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/

CVE-2015-3306 ProFTPD 1.3.5 Mod_Copy Command Execution | Rapid7. *Rapid7.com*. Retrieved 10 April 2018, from https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec

CVE-2010-2075 UnrealIRCD 3.2.8.1 Backdoor Command Execution | Rapid7. *Rapid7.com*. Retrieved 10 April 2018, from https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor