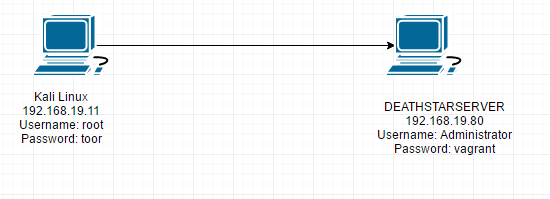
# In618 – Assignment 1

## Executive Summary:

This security audit summarizes the findings from an independent security review of the Death- Star Server. A total of four security vulnerabilities were discovered, all with a high severity level. These severe vulnerabilities can be easily exploited. These attacks resulted in a remote access shell as the root user and being able to upload a malicious file straight to the server. The system password file was extracted and the user’s passwords easily cracked due to weak passwords. Recommendations to improve security include updating the software described as a vulnerability in this report and to implement a strict password policy, a robust firewall to protect the server from potential attacks is also advised.

## Network Information:

The requested security audit consisted of the examination of a single server. A summary of the network configuration is displayed below:

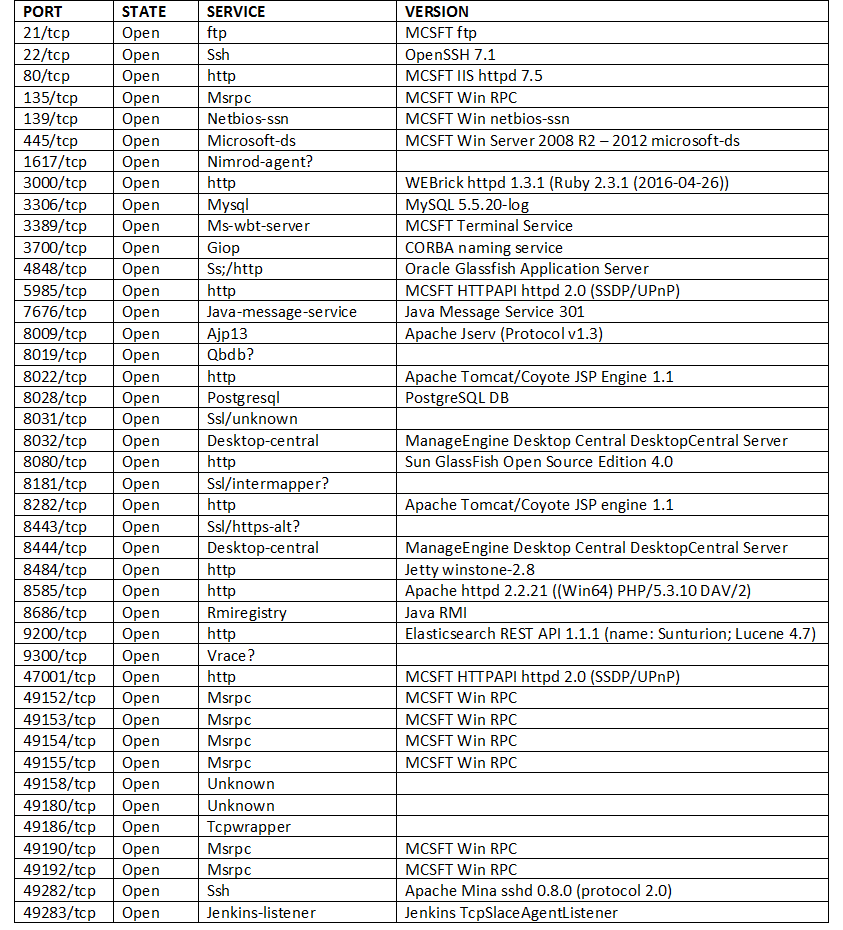


Additional information:

* Target hostname: DEATHSTARSERVER
* IP address: 192.168.19.80
* Target MAC address: 00:0C:29:85:30:95
* Operating System and version number: Microsoft Windows 7 2008 8.

## Open Ports and Running Services:

Thorough analysis of open network ports was performed using the nmap tool. All open networks are documented in the table below:



As displayed in the table above, there were 42 open network ports. The remaining 65493 ports were closed. A variety of common ports and services were open including:

* Http on ports 80, 3000, 5985, 8022, 8080, 8282, 8484, 8585, 9200, 47001
* Msrpc on ports 135, 49152, 49153, 49154, 49155, 49190, 49192

***Security recommendation***

Implement a strict software patching policy in the company’s general security policy. For example, set a policy to patch servers every week, or have an automated method to patch the applications running on the server.

## Vulnerability Assessment:

The security audit discovered several vulnerabilities that were discovered on the Death-Star server. Each vulnerability is outlined in the subsections below.

### Vulnerability 1: SMBv1

OpenVAS revealed a security vulnerability with the SMBv1 protocol running on port 445. The details of the service and the discovered vulnerability are listed below:

***Service Summary:***

* Protocol: SMBv1 Unspecified Remote Code Execution (Shadow Brokers)
* Software Name: SMBv1
* Software version: 5455
* Port number: 445

***Exploit Summary:***

* Exploit Name: auxiliary/server/capture/smb
* Exploit Result: Successful.
* Exploit Severity: High

***Security recommendation:***

Disable SMB v1 and/or block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

### Vulnerability 2: MS15-034

OpenVAS revealed a security vulnerability with the MS15-034 protocol running on port 80. The details of the service and the discovered vulnerability are listed below:

***Service Summary:***

* Protocol: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)
* Software Name: MS15-034
* Software version: 2646
* Port number: 80

***Exploit Summary:***

* Exploit Name: auxiliary/dos/http/ms15\_034\_ulonglongadd
* URL: https://www.rapid7.com/db/modules/auxiliary/dos/http/ms15\_034\_ulonglongadd
* Exploit Result: Successful.
* Exploit Severity: High
* CVE Number: CVE-2015-1635

***Security recommendation:***

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes from this link, <https://technet.microsoft.com/library/security/MS15-034>.

### Vulnerability 3: Microsoft Remote Desktop Protocol

OpenVAS revealed a security vulnerability with the Microsoft remote desktop protocol running on port 3389. The details of the service and the discovered vulnerability are listed below:

***Service Summary:***

* Protocol: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities
* Software Name: Microsoft Remote Desktop Protocol
* Software version: 4234
* Port number: 3389

***Exploit Summary:***

* Exploit Name: auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids
* URL: https://www.rapid7.com/db/modules/auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids
* Exploit Result: Successful.
* Exploit Severity: High
* CVE Number: CVE-2012-0002

***Security recommendation:***

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes from this link, <https://technet.microsoft.com/library/security/MS15-034>.

### Vulnerability 4: ManageEngine Desktop Central 9

OpenVAS revealed a security vulnerability with ManageEngine Desktop Central 9 protocol running on port 8022. The details of the service and the discovered vulnerability are listed below:

***Service Summary:***

* Protocol: ManageEngine Desktop Central 9 FileUploadServlet connectionID Vulnerability
* Software Name: ManageEngine Desktop Central 9
* Software version: 4402
* Port number: 8022

***Exploit Summary:***

* Exploit Name: exploit/windows/http/manageengine\_connectionid\_write
* URL: https://www.rapid7.com/db/modules/exploit/windows/http/manageengine\_connectionid\_write
* Exploit Result: Successful.
* Exploit Severity: High
* CVE Number: CVE-2015-8249

***Security recommendation:***

Update to ManageEngine Desktop 9 < build 90142

## Information Extraction

### User Credentials:

Remote access to the Death-Star system was accomplished and outlined in Section Vulnerability Assessment. After gaining remote access (as the root user) the /etc/shadow password file was easily extracted. Since the server operating system version is Windows 7, it is known that they use “salt” + “password” to generate the hash. All passwords are followed by the third colon, which indicates that the passwords are hashed with the NTLM algorithm.

|  |  |  |
| --- | --- | --- |
| **USERNAME** | **PASSWORD HASH** | **PASSWORD** |
| Administrator | e02bc503339d51f71d913c245d35b50b | vagrant |
| Admiral\_ozzel | 3f425836fcc62155d6a62124d2e66972 | iamclumsy |
| Admiral\_piett | 05df7a4296a2568fe35069d349eabbdd | stranglehold |
| Boba\_fett | 76ddfd40c995e2b8ad2c80cfd34226ef | Bountyhunter29 |
| Captain\_needa | ff6d31e7f258babb9f83e2064a4890f4 | Apology101 |
| Darth\_sidious | 91f6ebf1962689d8f5730f92217bb3f4 | darksideismine |
| Darth\_vader | 74c0a3dd06613d3240331e94ae18b001 | Daddy\_issues1 |
| Death\_star\_admin | d9ec08bd1fca158731bd08c9695304c1 | Deathstar313 |
| Emporer\_palpatine | cabcff2f0331a4b8bc1d09e91bd5e2de | darksideofmoon |
| General\_veers | f8302575356fecadea07ad9adf98be5b | toocloseforcomfort |
| Imperial\_guards | e5379c1cdb1205350a8fcdfcfb940f56 | fortheempire |
| Sshd\_server | 8d0a16cfc061c3359db455d00ec27035 | D@rj3311ng |
| Storm\_trooper\_1 | ca30e82ed0f55800878091a006493463 | Stormtrooper1 |
| Storm\_trooper\_2 | ab52004021277221ecd181bdcc28d9fa | stormtrooper |
| Storm\_trooper\_3 | 244defe0ccb72637349e6ab32742eefb | Stormtrooper96 |
| Storm\_trooper\_4 | 8676b47ff5d0679538d6ee543de83a10 | supertrooper |
| Storm\_trooper\_5 | 64942e6abcb33097d488f74ffeb671cc | 20cute kittens07 |
| vagrant | 7e5a133840b3129c6ce8a379d046fb2f |  |

Although the method to crack the passwords was “offline” (e.g., download the password file and decrypt) and “online” attack could also be conducted using a tool such as Hydra or Armitage. This means that an attacker may not need root access to the machine to break the weak passwords.

### Death Star information

From searching through the files of the Death Star system I discovered the following files:

**On the Stormtrooper 2 user account:**

* deathstar-darthvader-secretinfo.txt (this file contained knowledge about Darth Vader’s user account details)
* ace\_of\_hearts.jpg
* four\_of\_clubs.mp3
* jack\_of\_hearts.docx
* seven\_of\_spades.pdf
* ten\_of\_diamonds.png

**On the Administrator user account:**

* ace\_of\_hearts.jpg
* four\_of\_clubs.mp3
* jack\_of\_hearts.docx
* seven\_of\_spades.pdf
* ten\_of\_diamonds.png

***Security recommendation***

Immediately change ALL passwords in the system. The currently used passwords are weak; for example, the stormtrooper 2 password was ‘stormtrooper’, which would be one of the first guesses an attacker would try. A password policy should be implemented at the Death-Star to enforce creation on complex passwords (e.g., alphanumeric and symbols) and to enforce every user to change their password at least every 2 months. A better hashing algorithm is also advised, possibly SHA254 or BCrypt.

## Conclusions:

This report summarized the findings from an independent security audit of the Death-Star server. A total of four vulnerabilities were discovered. The severity of these vulnerabilities were all high. All were practically exploited against the target system and root access and uploading a malicious file was obtained. This is a high security risk and immediate action needs to be taken to mitigate the potential risk to the information stored on and services provided by the server. The security recommendations specified in the report should be implemented and then another security audit should be performed to re-assess the security of the server.