Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:  
Datum:

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

**1. CVE-2015-3306**

1.1 **Informacije o ranljivosti**ID ranljivosti (CVE): CVE-2015-3306  
Pogođen servis: ProFTPD  
CVSS ocena: 10

Severity: Critical  
Opis ranljivosti: Mod\_copy modul u ProFTPD 1.3.5 dozvoljava udaljenim napadačima da čitaju i pišu u proizvoljne datoteke putem komandi "site cpfr" i "site cpto".

1.2 **Opis eksploita**Izvor eksploita: Metasploit (unix/ftp/proftpd\_modcopy\_exec)  
Metod eksploatacije:  
Ovaj modul koristi SITE CPFR/CPTO mod\_copy u ProFTPD verziji 1.3.5. Klijent koji nije autentifikovan može iskoristiti ove komande za kopiranje datoteka sa bilo kog dela sistema na izabrano odredište. Komande za kopiranje se izvršavaju sa pravima ProFTPD servisa, koja podrazumevano radi pod privilegijama nobody korisnika. Koristi se /proc/self/cmdline za kopiranje PHP payload-a cime se omogucava remote izvrsavanje PHP koda.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija ProFTPD bude 1.3.5 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

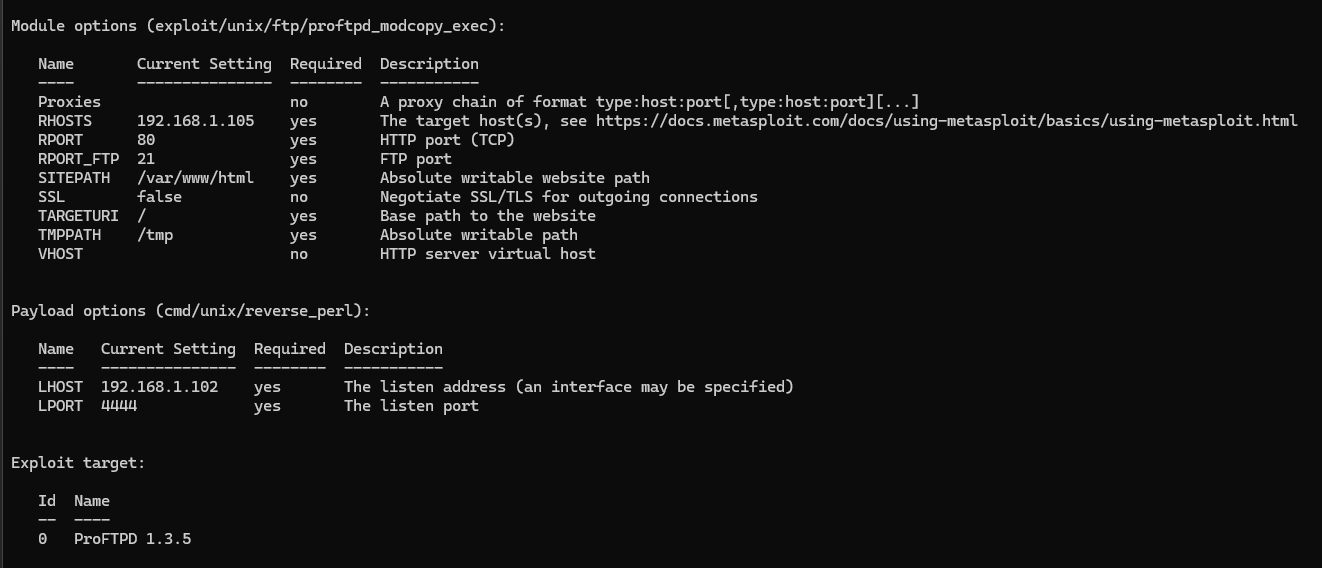
2.2 **Koraci eksploatacije**Objasnite proces eksploatacije korak po korak - DETALJNO:

Link do repozitorijuma sa exploitom: <https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/unix/ftp/proftpd_modcopy_exec.rb>

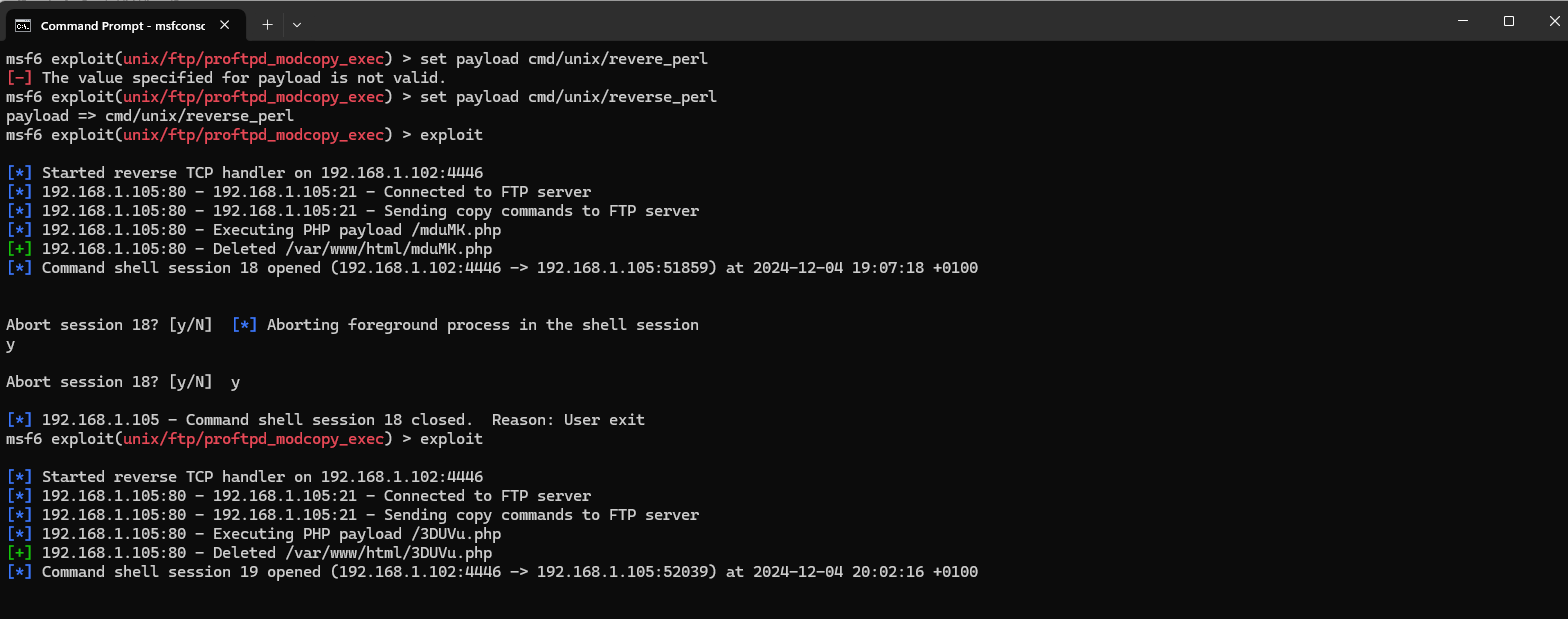
Nakon što smo podesili Metasploitable3 virtualnu mašinu (detalji u prošloj sekciji) potrebno je pokrenuti Metasploit command line tool na host mašini. Zatim se pokreću sledeće komande:

search CVE-2015-3306 > use unix/ftp/proftpd\_modcopy\_exec > options > set rhost 192.168.1.105 > exploit

Prvo se kopira PHP payload u tmp datoteku. PHP payload izvrsava komandu koja mu se prosledi kroz GET parametar. Pomocu SITE CPFT i CITE komandi se payload kopira u web direktorijum odakle se moze pokrenuti kroz http zahtev. Exploit onda salje zahtev na url do payloada i prosledjuje mu komandu koju treba da izvrsi.



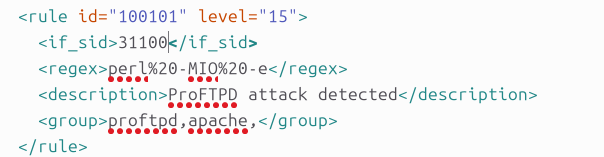
2.3 **Rezultat eksploatacije**Prikažite rezultate eksploatacije:



Detekcija Korišćenjem Wazuh SIEM-a

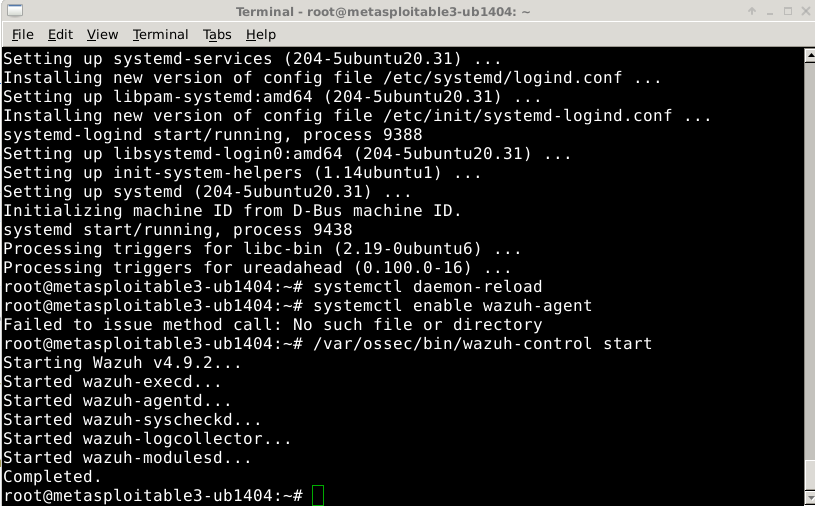
Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM pravila**Pravila korišćena za detekciju:  
ID pravila: 100101  
Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja izvrsavanje perl skripte. 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.



3.2 **Konfiguracija SIEM-a**Podešavanje Wazuh agenta:

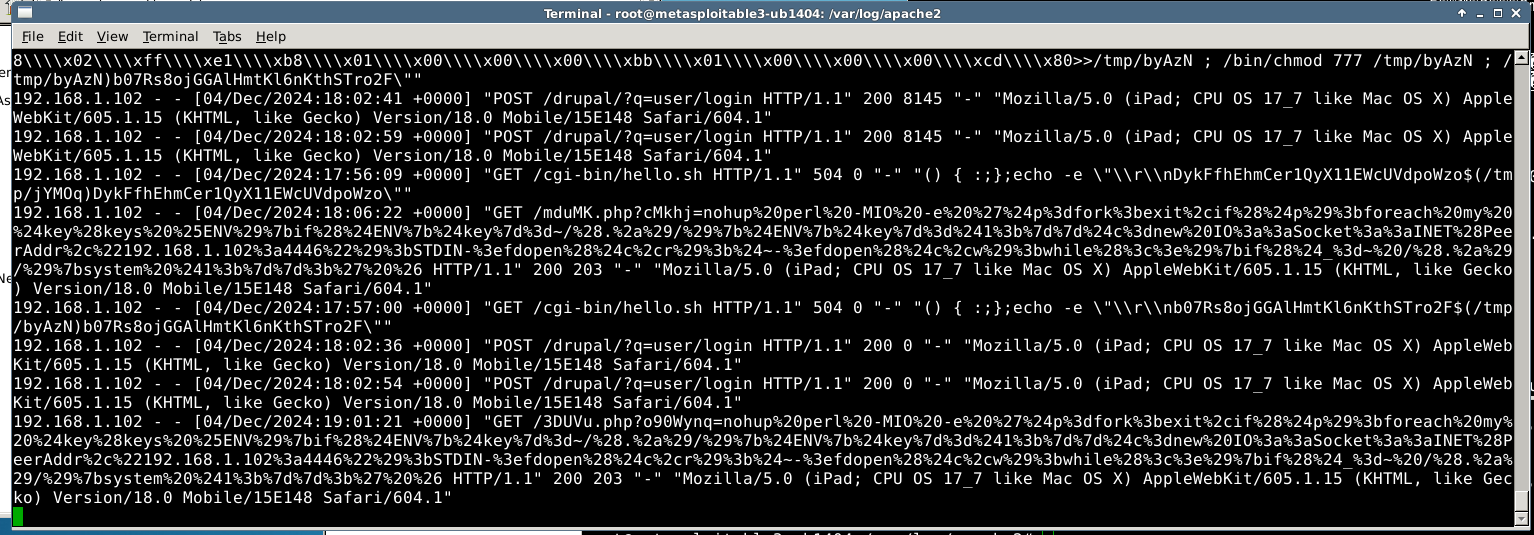
Na target mašini je instaliran Wazuh-Agent i podešena je env varijabla (**WAZUH\_MANAGER="192.168.1.104" apt-get install wazuh-agent**) koja kreira vezu između agenta i Wazuh Manager-a.

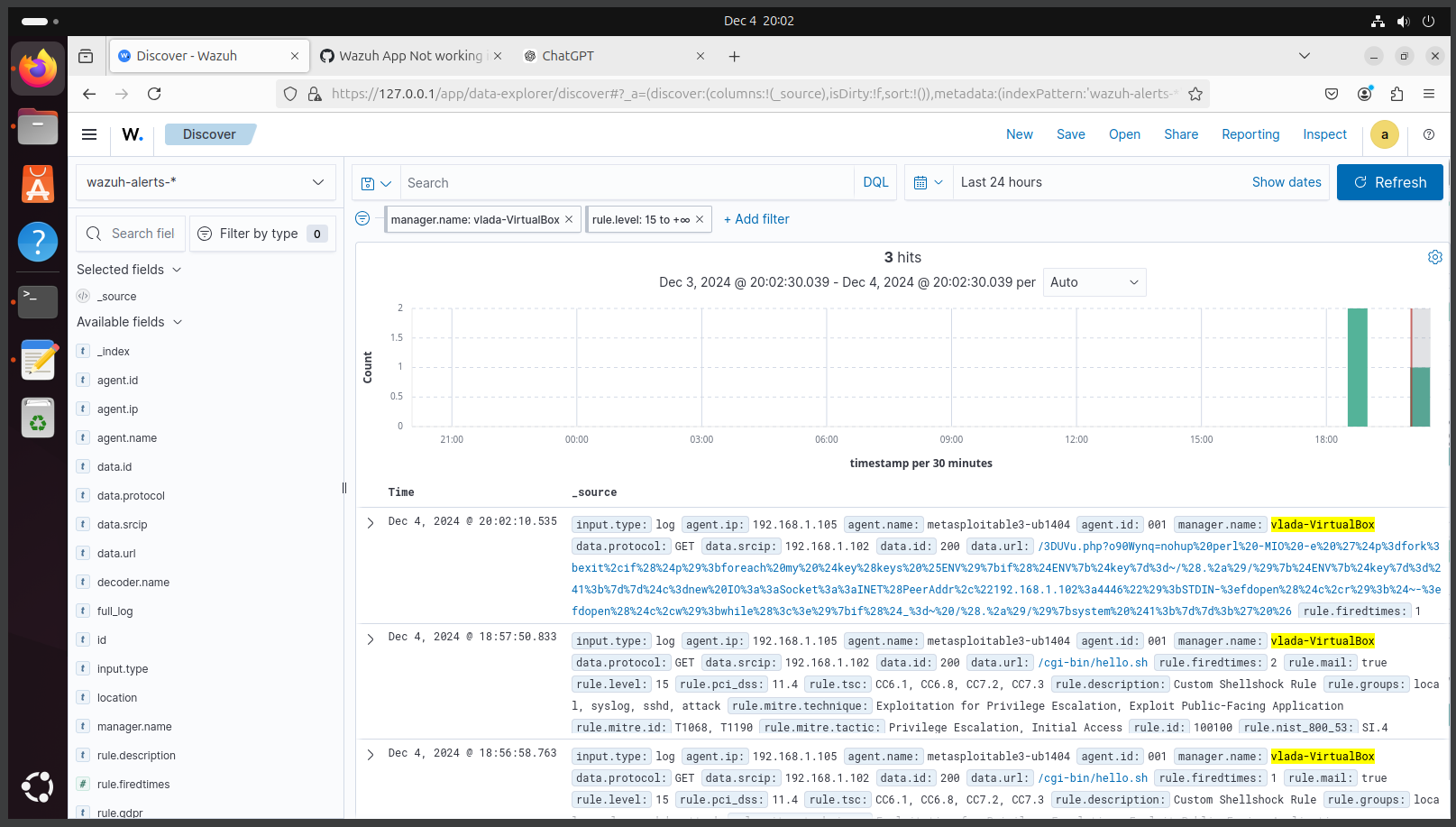


Prikupljanje logova:  
Prikupljaju se svi logovi generisani od strane Apache2 servera sa putanje: **/var/log/apache2/access.log**

3.3 **Proces detekcije**Opišite proces detekcije:

Primetiti sledeci log koji sadrzi perl MIO –e komandu.



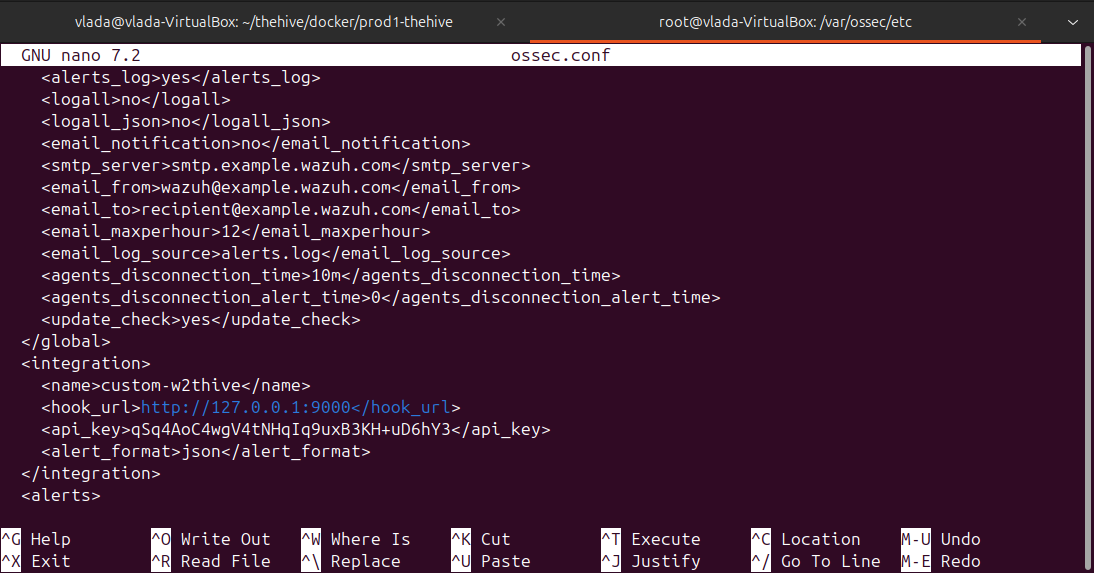


*Podaci o detektovanom napadu unutar Wazuh interfejsa*

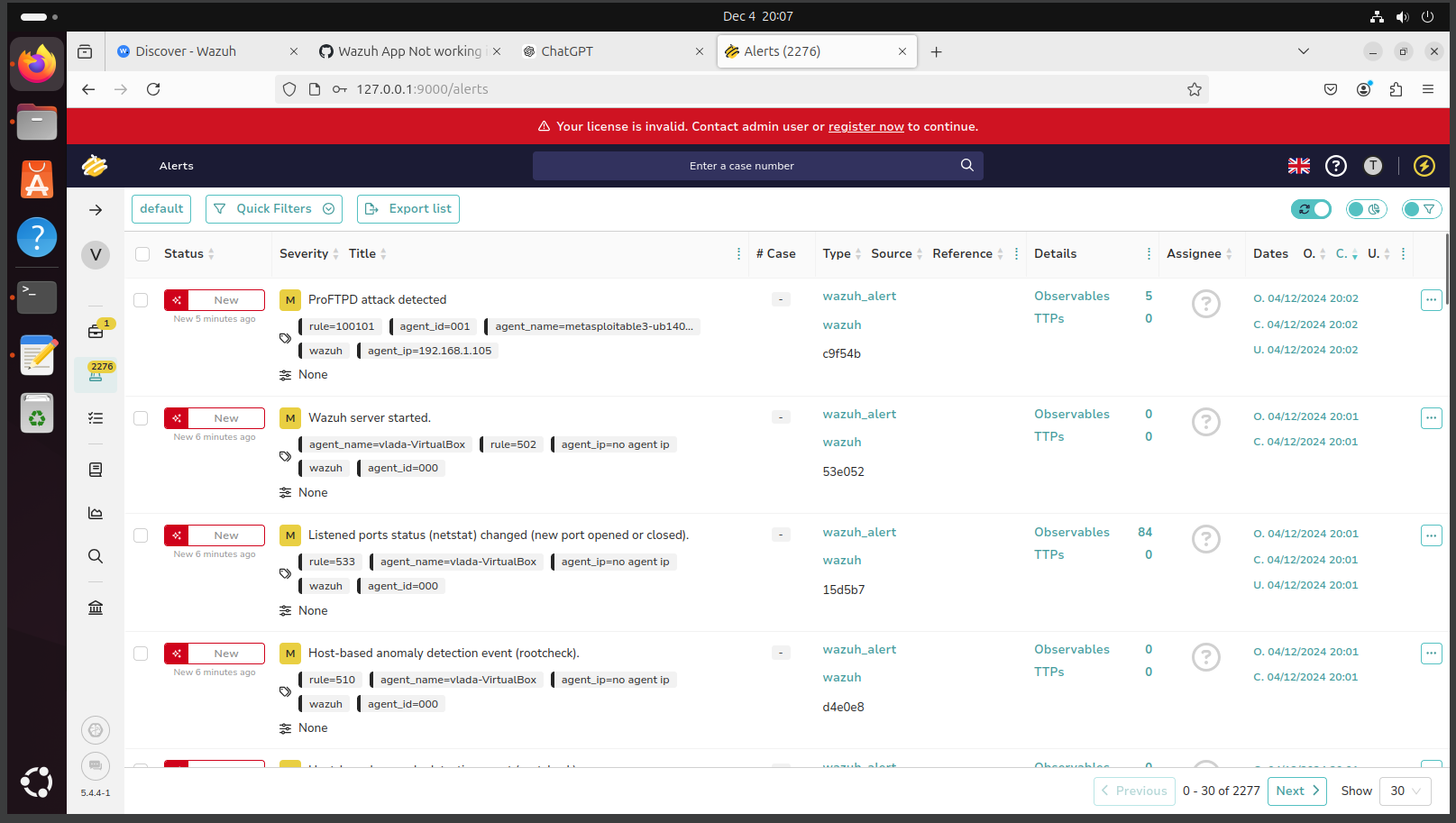
Incident Response sa The Hive-om

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:  
