Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:  
Datum:

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

**1.** [**CVE-2010-2075**](https://www.tenable.com/cve/CVE-2010-2075)

1.1 **Informacije o ranljivosti**ID ranljivosti (CVE): CVE-2010-207  
Pogođen servis: UnrealIRCD  
CVSS ocena: 10

Severity: Critical  
Opis ranljivosti: Udaljeni IRC server koristi verziju UnrealIRCd koja ima backdoor, što omogućava napadaču da izvrši proizvoljan kod na pogođenom hostu.

1.2 **Opis eksploita**Izvor eksploita: Metasploit (unix/ircd/unreal\_ircd\_3281\_backdoor)  
Metod eksploatacije:  
Nakon uspostavljanja veze i dobijanja bannera sa servera (što je uobičajena informacija o verziji i konfiguraciji servera), exploit šalje komandnu koja počinje sa „AB;“ a zatim sa kodiranim payload-om. Taj niz aktivira zadnja vrata na serveru i omogućava izvršavanja proizvoljnog koda.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija Unrealircd bude 3.2.8.1 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

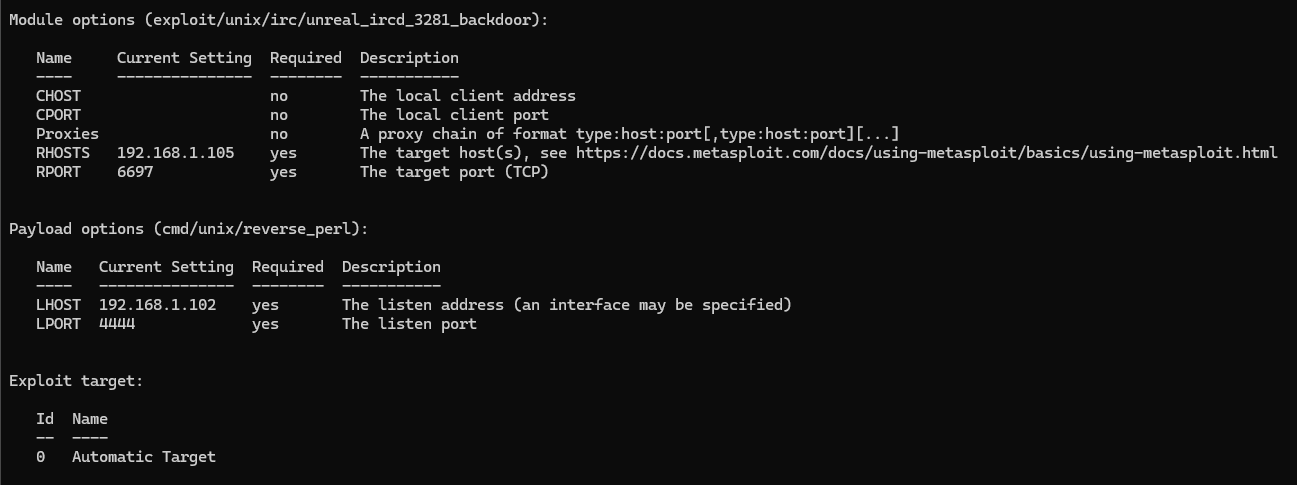
2.2 **Koraci eksploatacije**

Link do repozitorijuma sa exploitom: <https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/irc/unreal_ircd_3281_backdoor.rb>

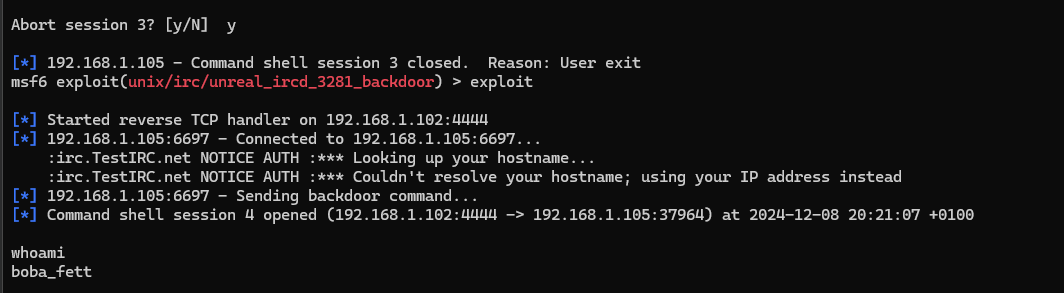
Nakon što smo podesili Metasploitable3 virtualnu mašinu (detalji u prošloj sekciji) potrebno je pokrenuti Metasploit command line tool na host mašini. Zatim se pokreću sledeće komande:

search unrealircd > use unix/ircd/unreal\_ircd\_3281\_backdoor > options > set rhost 192.168.1.105 > set rport 6697 > exploit

Exploit salje zahtev koji pocinje sa AB; za cime ide payload. Payload sadrzi skriptu za otvaranje sesije prema host racunaru.



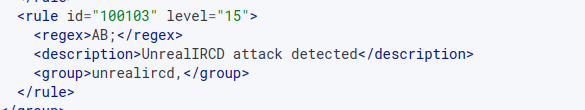
2.3 **Rezultat eksploatacije**Prikažite rezultate eksploatacije:



Detekcija Korišćenjem Wazuh SIEM-a

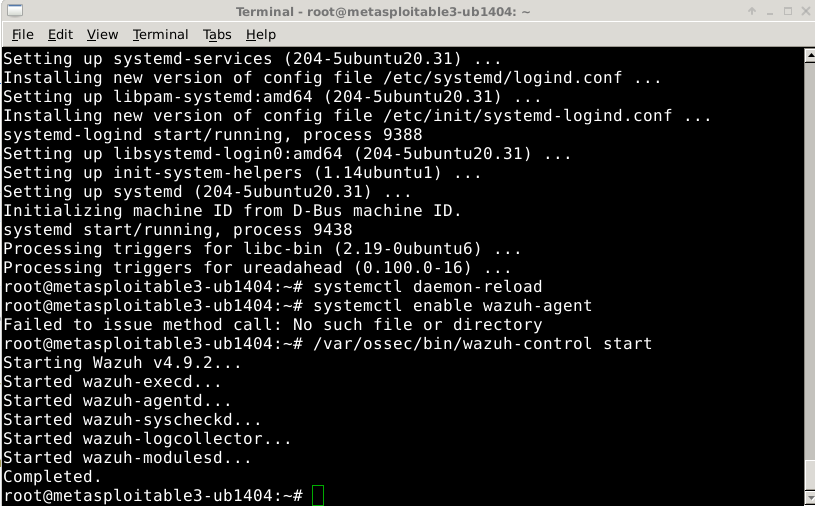
Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM pravila**Pravila korišćena za detekciju:  
ID pravila: 100103  
Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja kljucne karaktere iza kojih se izvrsava proizvoljni kod. To su karakteri **AB;**. 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.

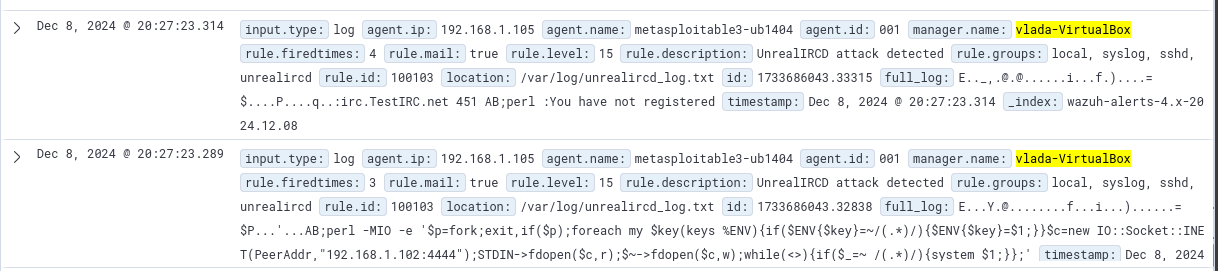


Prikupljanje logova:  
Prikupljaju se logovi generisani pomocu tcpdump:

**/var/log/unrealircd\_log.txt**

3.3 **Proces detekcije**Opišite proces detekcije:

Primetiti sledeci log koji sadrzi **AB;** kljucne karaktere za backdoor.

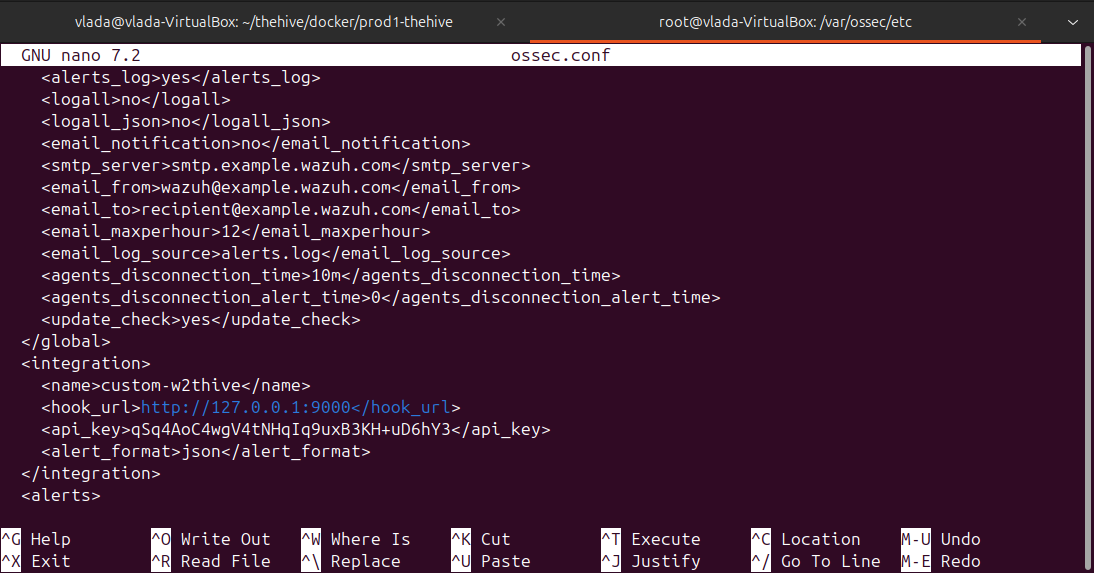


*Podaci o detektovanom napadu unutar Wazuh interfejsa*

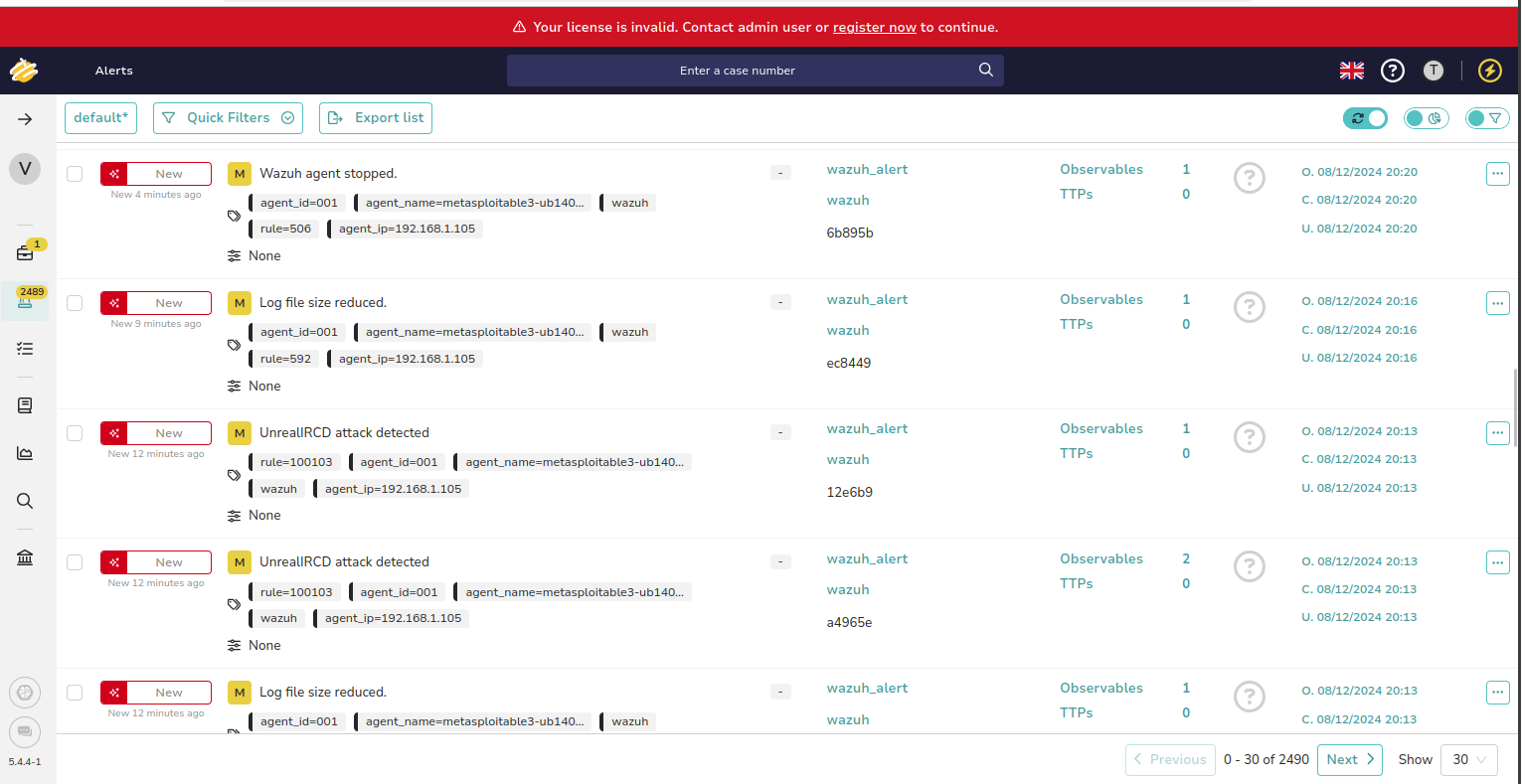
Incident Response sa The Hive-om

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:  
