Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Anastasija Savić i Katarina Vučić
Datum: 30.11.2024.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**

ID ranljivosti (CVE): CVE 2014-6271
Pogođen servis: GNU Bash
CVSS ocena: 10.0 (kritično)
Opis ranljivosti: Omogućava napadačima da izvrše proizvoljan kod u ciljanom sistemu. Napdač može, prilikom korišćenja bash-a, umetnuti maliciozan kod u env (environment variable). Napad se može izvršavati udaljeno. Bash se široko koristi, u aplikacijama na Unix/Linux sistemima, uključujući web servere poput Apache-a, gdje CGI skripte mogu pokrenuti ranjiv kod.
(Uključite kratak opis ranljivosti, pogođeni servis i severity)

1.2 **Opis eksploita**

Izvor eksploita:
(Link ka public available eksploitu ili naziv metasploit modula)

https://www.rapid7.com/db/modules/exploit/multi/http/apache_mod_cgi_bash_env_exec/
Metod eksploatacije:
(kratak opis principa kako exploit radi)

VSFTPD (Very Secure FTP Daemon) verzija 2.3.4 sadrži backdoor ranjivost koja omogućava napadačima da dobiju pristup udaljenom sistemu sa privilegijama root korisnika. Ova ranjivost nije greška u kodu, već je rezultat zlonamjerne modifikacije softvera, gdje je ubačen backdoor. Backdoor se aktivira kada napadač koristi ime koje sadrži ,,🙂”. Na primjer: ,,user:)”. Kada se unese takvo korisničko ime, aktivira se maliciozni kod. Kod otvara TCP port 6200 na kojem se pokreće interaktivni shell sa root privilegijama. Omogućena je direktna kontrola nad ciljanim sistemom.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**

Ranjiv cilj:

(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)
Ciljna mašina je Ubuntu 14 na kojoj je instalirana ranjiva verzija VSFTPD servisa.

Verzija servisa: v2.3.4.

Port: 21.

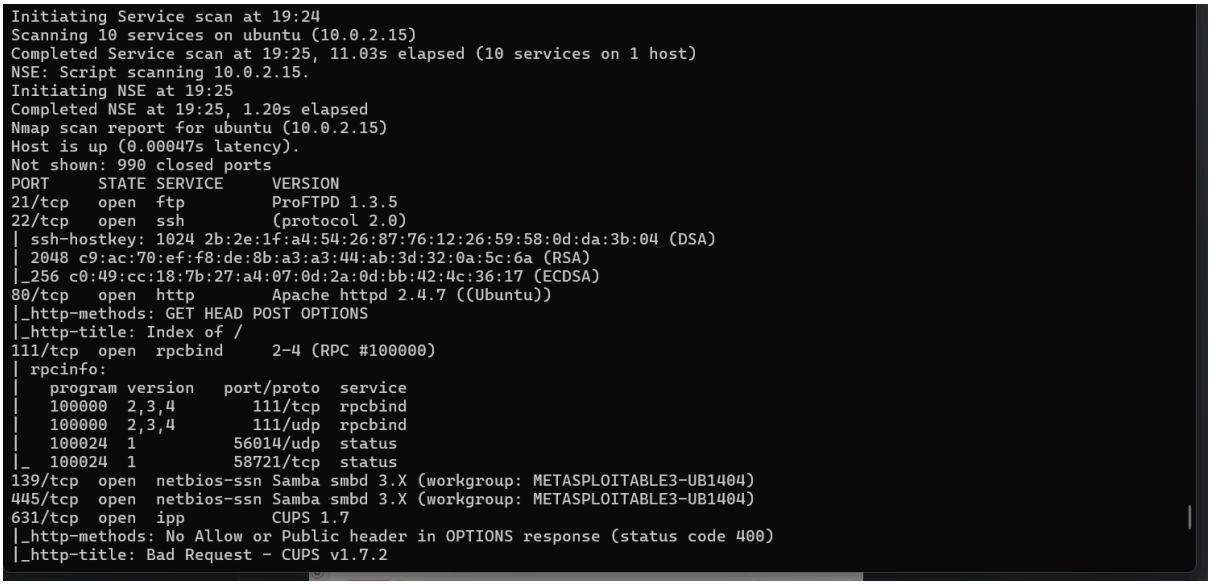
Alati za eksploataciju:

(Metasploit ili neki drugi alat, Python skripta, Perl skripta…)

Korišćen je Metasploit alat za detekciju i eksploataciju ranjivosti.

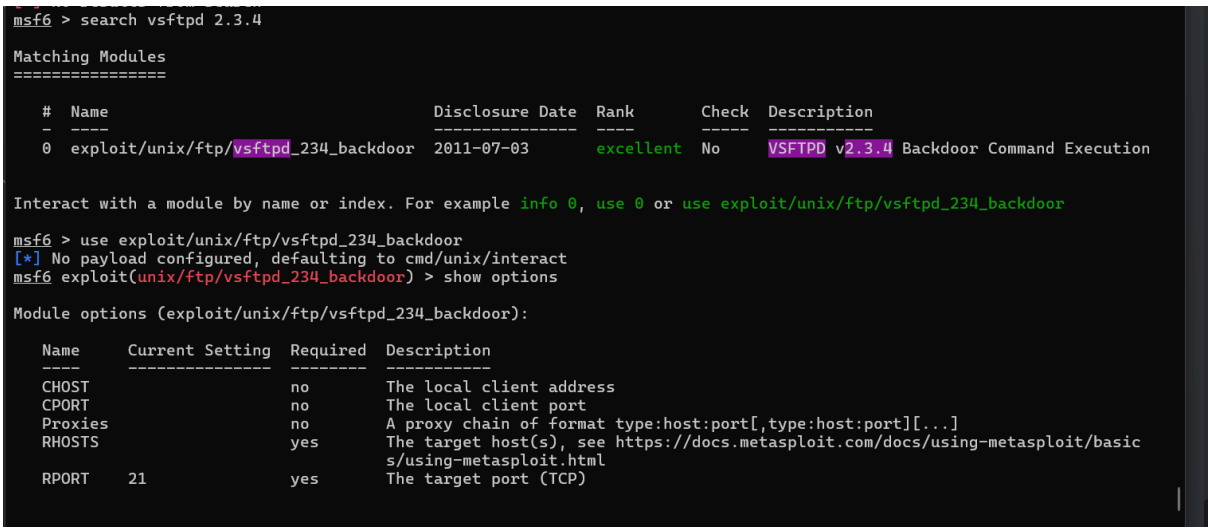
2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak - DETALJNO:
(Uključite screenshot-ove celog procesa)

Na *Slici 1* ispod vidimo skeniranje ubuntu servisa koji trče na odgovarajućoj adresi. Možemo vidjeti da na portu 21 trči ftp servis.



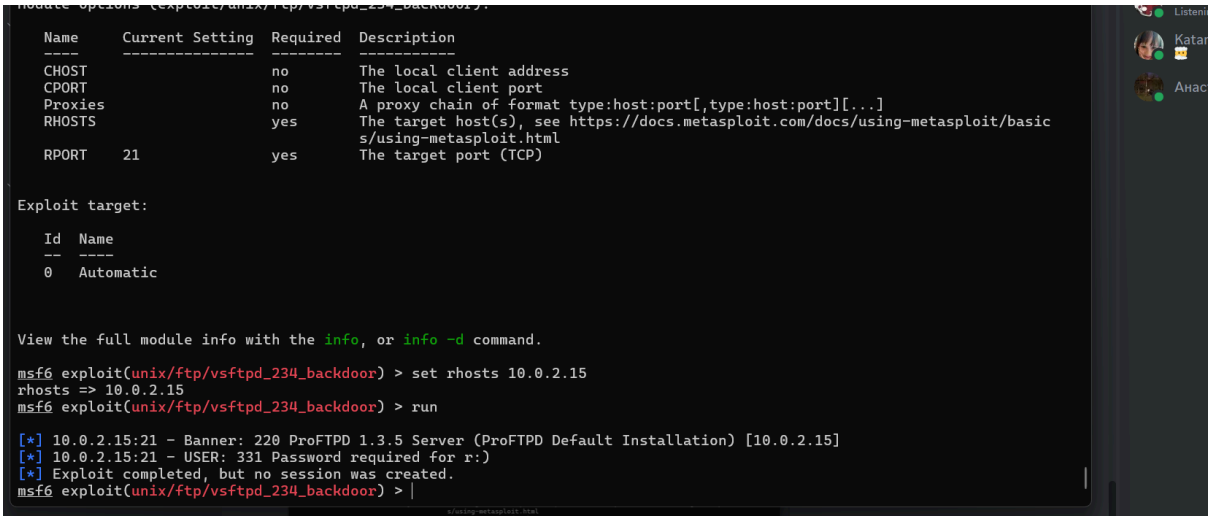
Slika 1

Nakon toga smo pretražili koji ekspoliti postoje (uz pomoće metasploit alata). To se radi koristeći ***serach*** komandu. Nakon toga navodimo servis za koji tražimo eksploit. U našem slučaju je to ***search vsfptd 2.3.4*** komanda. Nakon što izaberemo koji ćemo eksploit koristiti koristimo komandu ***use naziv eksploita***. Za prikaz konfiguracionih opcija koje će odabrani eksploit koristiti, koristimo ***show options*** komandu.



Slika 2

Slika 3 prikazuje kako smo podesili RHOST atribut. Nakon toga smo uradili ***run*** eksploita.



Slika 3

2.3 **Rezultat eksploatacije**

Prikažite rezultate eksploatacije:

Slika 3 prikazuje rezultat eksploatacije.

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM eravila**

Pravila korišćena za detekciju:

(Navedite specifična Wazuh pravila koja su se aktivirala ili prilagodila za detekciju eksploita)

ID pravila:

(Uključite ID pravila i kratak opis)

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:

(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)

Agent se nalazi na istoj mašini kao i metasploitable3. Ta mašina je Ubuntu 14. U terminalu run-nujemo komande koje dobijemo nakon što deploy-ujemo agenta sa Wazuh servera. Komande su prilagođene mašini na kojoj će biti agent, ip adresi i nazivu manager-a. Nakon toga samo startujemo wazuh agenta - komanda ***sudo service wazuh-agent start***. Takođe, možemo koristiti komande ***sudo service wazuh-agent restart*** i ***sudo service wazuh-agent stop*** za ponovno pokretanje i zaustavljanje wazuh agenta.

Prikupljanje logova:

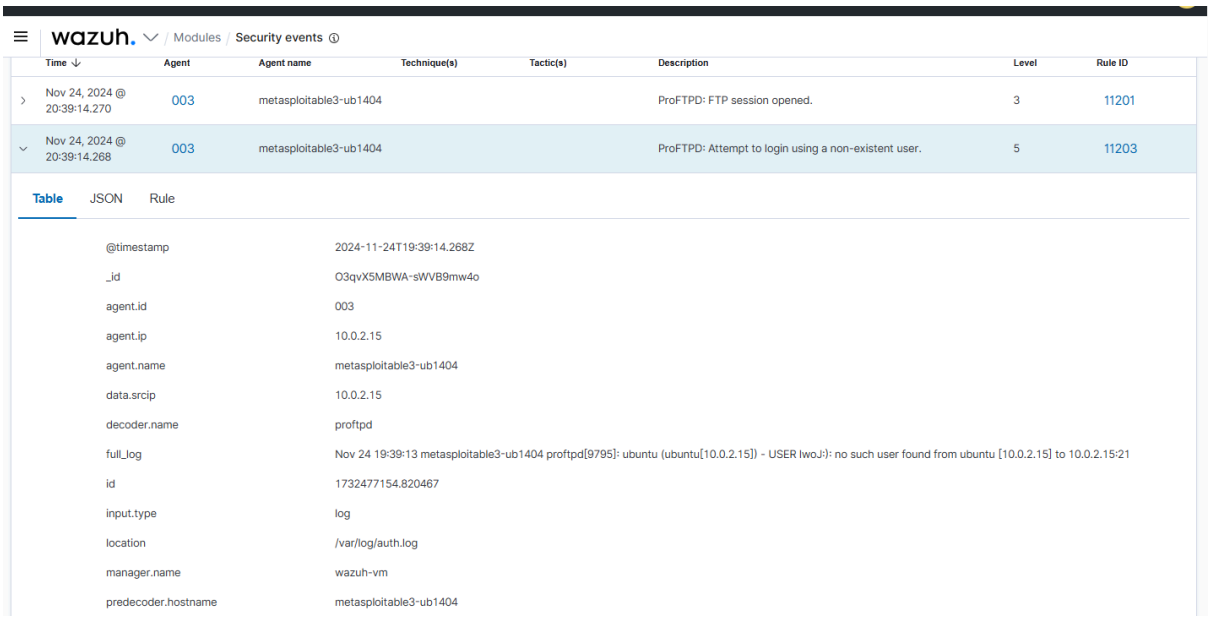
(Navedite koje logove pratite da biste otkrili pokušaje eksploatacije)

Pokušaji eksploatacije se mogu vidjeti na *Slici 6.* Logovi nam prikazuju informacije o pokušaju ekspolatacije (koja eksploatacija je u pitanju, kada je pokušaj izveden, sa kog agenta i mašine itd. (pogledati *Sliku 6*).

3.3 **Proces detekcije**

Opišite proces detekcije:

(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha) - *Slika 4*



Slika 4

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

Opis integracije:

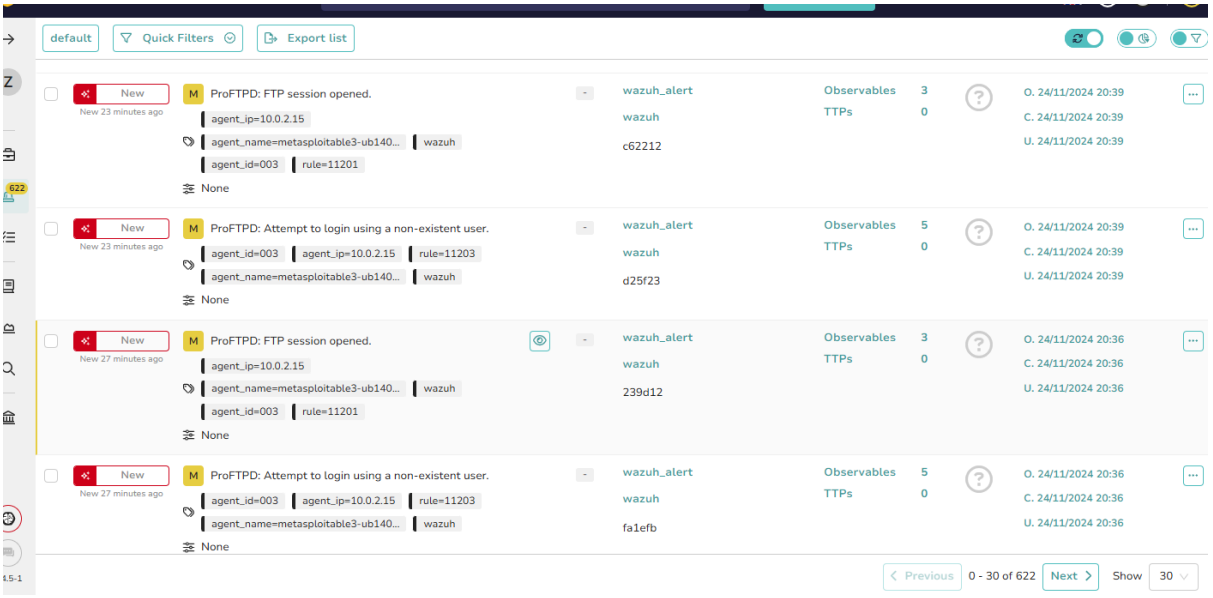
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)

Wazuh i TheHive su povezani prateći tutorijal sa linka https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/

Integracija pravila:

(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a - *Slika 6.*



Slika 6

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

Detalji o slučaju:

(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)