Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Milica Đumić  
Datum: 05.12.2024.

Pregled Ranljivosti

* 1. **Informacije o ranljivosti**

**ID ranljivosti (CVE):** CVE-2006-5815

**Pogođen servis:** ProFTPD

**CVSS ocena:** 10

**Opis ranljivosti:**

Prekoračenje vrednosti bafera zasnovano na steku. Ranjivost je pronađena u funkciji sreplace u ProFTPD-u, u verzijama 1.3.0 i ranijim. Napadači su najčešće autentifikovani, a uspešno sproveden napad izaziva pad sistema ili izvršavanje malicioznog koda.

* 1. **Opis eksploita**

**Izvor eksploita:**

Ekspolit je dostupan na sledećem linku: <https://www.exploit-db.com/exploits/16852>.

**Metod eksploatacije:**

Ranjivost je nađena u funkciji *sreplace* u datoteci *src/support.c*. U ovom eksploitu se koristi prelivanje bafera zaslovano na prelivanju od jednog do drugog u gomili. Postoje najmanje dve greške u pomenutoj funkciji: prelivanje gomile od jednog do drugog i prekoračenje bafera na bazi steka.

Proces Eksploatacije

2.1 **Podešavanje eksploita**

**Ranljiv cilj:**

U pitanju je *metasploitable*3 ranjiva mašina. ProFTPD mora biti verzija 1.3.0 ili neka ranija verzija. Port pogođen u ovom eksploit je 21.

**Alati za eksploataciju:**

Korišćen je *Metasploit* alat za eksploataciju ranjivosti. Odabran je eksploit pod nazivom: *ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux).*

2.2 **Koraci eksploatacije**

Prvobitno se pokreće *Metasploit,* iz terminala sa administratorskim privilegijama, uz pomoć komande *msfconsole.bat.*

cd C:\metasploit-framework\bin

msfconsole.bat

Zatim se pronađe prethodno opisani eksploit i odabere (*search* i *use*).

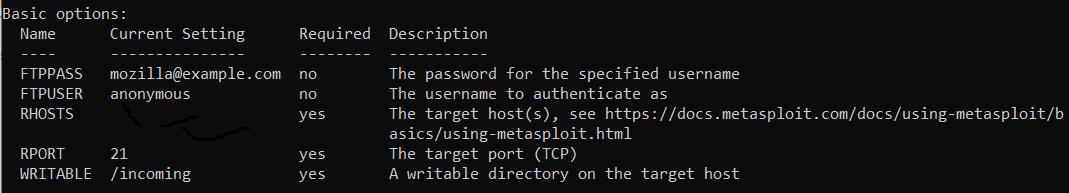
search cve-2006-5815

0 exploit/linux/ftp/proftp\_sreplace

1 \\_ target: Automatic Targeting

use 1

Nakon toga se pomoću komande *info* mogu pronaći dodatne informacije u vezi obaveznih i opcionih parametara samog eksploita. U nastavku će biti inicijalizovani obavezni parametri.

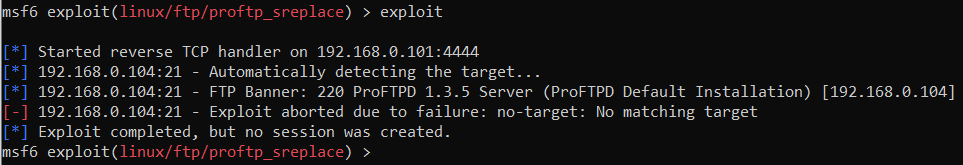


Neophodno je podesiti IPadresu ranjive mašine.

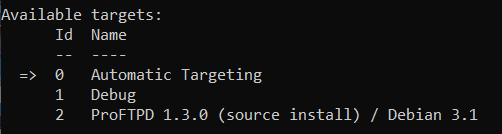
set rhosts 192.168.0.104

2.3 **Rezultat eksploatacije**

Pokretanje eksploita se vrši komandom *exploit*:



Izvršeno je više eksploita, razlika je bila u target-u. Sve opcije (iz snimka CMD-a priloženog ispod) su isprobane, ali su završene na isti način. Nezavisno od toga, eksploit je aktivirao dva SIEM pravila (navedena u narednom poglavlju) zasnovana na napadu ProFTPD-a.



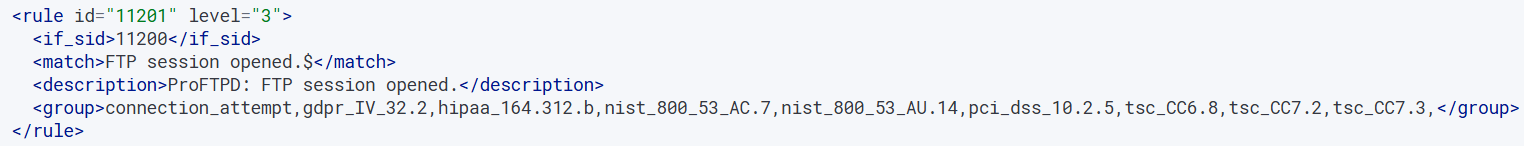
Detekcija Korišćenjem Wazuh SIEM-a

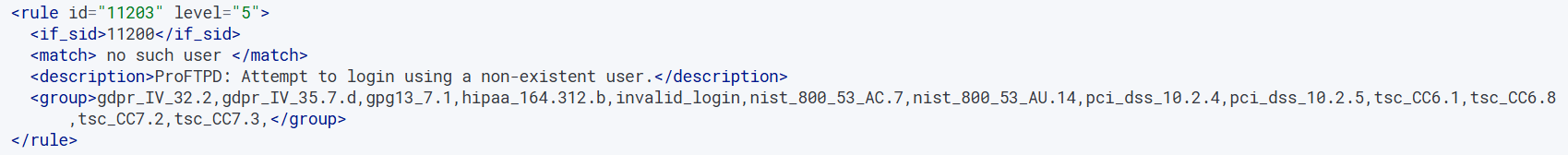
3.1 **Wazuh SIEM pravila**

**Pravila korišćena za detekciju:**

Konkretno su iskorišćena 2 pravila: prvo pravilo proverava da li je ProFTPD sesija otvorena, dok drugo korišćeno pravilo hvata pokušaj logovanja sa neispravnim kredencijalima.

**ID pravila:** 11201 i 11203.





3.2 **Konfiguracija SIEM-a**

**Podešavanje Wazuh agenta:**

Podešavanje započinje u *Wazuh* menadžeru. Sam *Wazuh dashboard* je moguće otvoriti putem *browser-a* na adresi [*http://ip\_adresa\_menadžera:443*](http://ip_adresa_menadžera:443)ukoliko je server vidljiv iz lokalne mašine. Potrebno je ući u meni *Server Management > Endpoints Summary > Deploy new agent*, zatim izabrati opciju *Linux RPM amd64* i uneti IP adresu *Wazuh* menadžera. Ovim postupkom se izgenerišu potrebne komande za konfiguraciju ranjive mašine.

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.9.2-1\_amd64.deb && sudo WAZUH\_MANAGER='172.29.200.157' dpkg -i ./wazuh-agent\_4.9.2-1\_amd64.deb

/var/ossec/bin/wazuh-control start

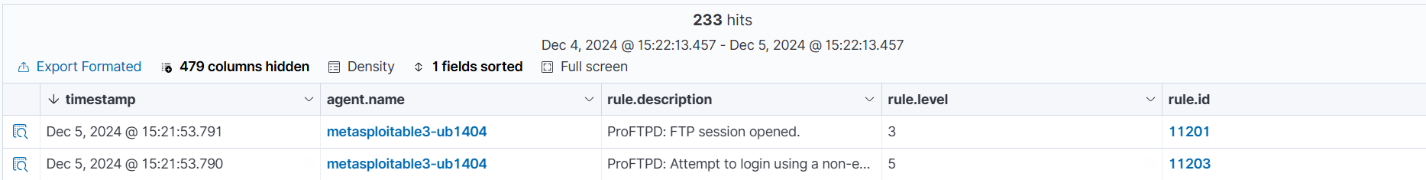
Pokretanjem ovih komandi *Wazuh* agent je uspešno podešen.

**Prikupljanje logova:**

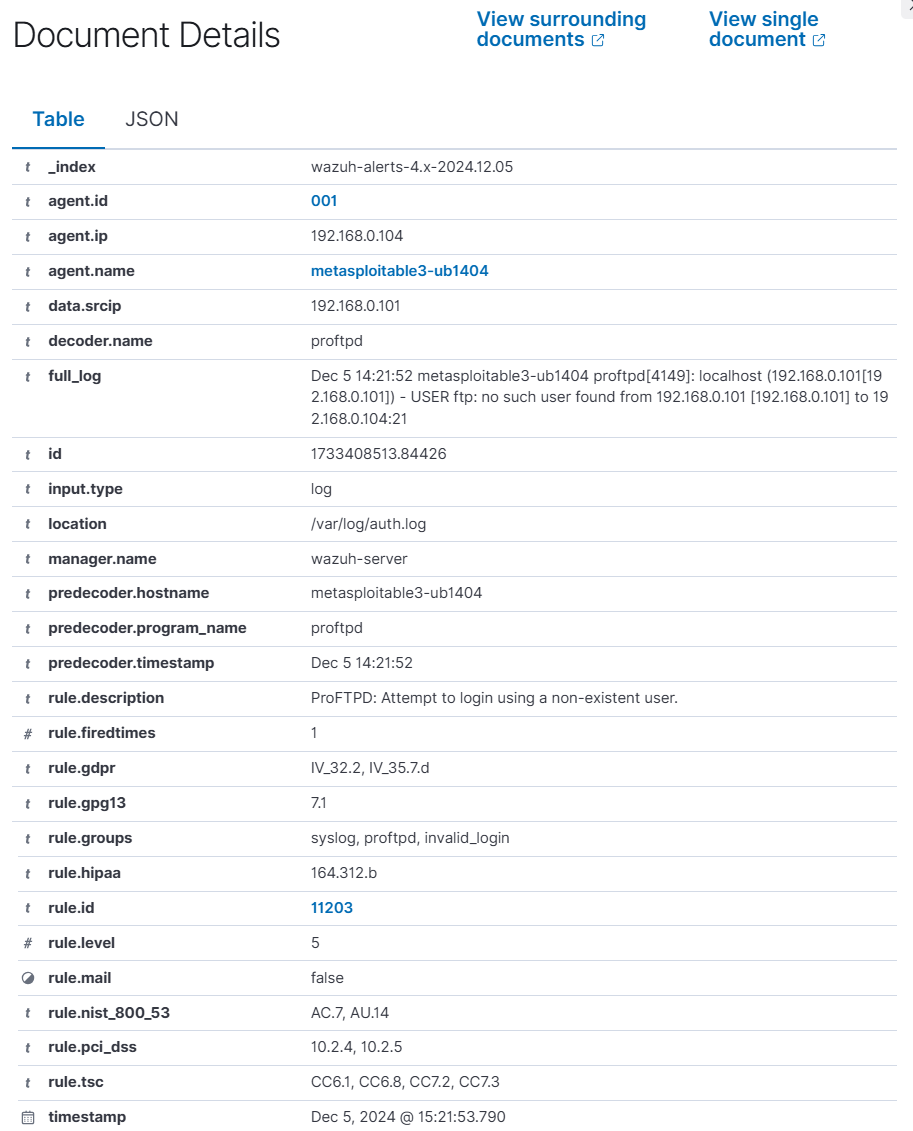
Koriste se sistemski *(/var/log/syslog*) i logove *(/var/log/auth.log*) za utorizaciju. Sitemski log je potreban za detekciju uspostavljanja FTP sesije, a logovi za utorizaciju se koriste kako bi se detektovalo logovanje sa pogrešnim kredencijalima.

3.3 **Proces detekcije**

U sekciji *Wazuh* menadžera *Threat Intelligence >* *Threat Hunting* je moguće uočiti dve pretnje koja se tiču *ProFTP-a* što je bio cilj.







Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

**Postupak u *TheHive-u***

Ukoliko je prethodno instaliran *Docker*, instalacija *TheHive-a* se može jednostavno obaviti pokretanjem komande:

docker run -d --rm -p 9000:9000 strangebee/thehive:5.4.5-1

Nakon što je instaliran *TheHive* potrebno je napraviti organizaciju sa administratorskim nalogom. Zatim kreirati korisnika uz administratorske permisije koji je dodeljen toj organizaciji. Njemu je potrebno dodati lozinku kako bi mogao da se prijavi. Tako kreiran korisnik ima mogućnost da kreira nove korisnike, upravlja slučajevima i uzbunama. Integracija sa *Wazuh-om* je moguća *pomoću TheHive REST API-a*. Za potrebe ovoga kreiramo korisnika sa permisijama *„analyst*“ i za njega generišemo *API* ključ.

**Postupak u *Wazuh menadžeru***

Ukoliko *Wazuh* menadžer prethodno nije instaliran, dovoljno je [preuzeti .ova sliku](https://documentation.wazuh.com/current/installation-guide/index.html) i importovati je u alat za pokretanje virtuelnih mašina (npr. *Oracle VirtualBox*).

Potrebno je instalirati python modul za *TheHive*, komandom:

sudo /var/ossec/framework/python/bin/pip3 install thehive4py==1.8.1

Sledeći korak je kreirati python skriptu na putanji */var/ossec/integrations/custom-w2thive.py.* Vrednost *lvl\_threshold* unutar skripte odgovara minimalnom *level-u* upozorenja koji će biti prosleđen *TheHive-u*. Postavka *lvl\_threshold-a* na 0 obezbeđuje registrovanje svih događaja. Potrebno je napraviti i bash skriptu u istom direktorijumu sa nazivom *custom-w2thive.* Ona će će pokrenuti *custom-w2thive.py*.

Potrebno je još dodeliti adekvatne permisije *Wazuh-u* tako što unosimo sledeće komande:

sudo chmod 755 /var/ossec/integrations/custom-w2thive.py

sudo chmod 755 /var/ossec/integrations/custom-w2thive

sudo chown root:wazuh /var/ossec/integrations/custom-w2thive.py

sudo chown root:wazuh /var/ossec/integrations/custom-w2thive

Što se tiče integracije pravila, da bismo obezbedili da se izvrši integraciona skripta neophodno je da u */var/ossec/etc/ossec.conf* unesemo sledeći kod:

<ossec\_config>

…

<integration>

<name>custom-w2thive</name>

<hook\_url>http://192.168.0.100:9000</hook\_url>

<api\_key>vBewU6WoZ2KaPWGgEGjToJnPHi/ASBmL</api\_key>

<alert\_format>json</alert\_format>

</integration>

…

</ossec\_config>

Na kraju je potrebno restartovati *Wazuh* menadžera, a to postižemo komandom:

sudo systemctl restart wazuh-manager

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

**Detalji o slučaju:**



