Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:Spasoje Brboric

Datum: 11.12.2024.

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE-2015-3306

Pogođen servis: ProFTPD (mod_copy modul)

CVSS ocena: 10.0 Opis ranljivosti:

Ranjivost CVE-2015-3306 pogađa ProFTPD servere koji imaju omogućeni modul mod_copy. Ova ranjivost omogućava lokalnim ili daljinskim napadačima da zloupotrebe komandni skup ovog modula kako bi kopirali datoteke iz ili u direktorijume kojima server ima pristup. Korišćenjem ove ranjivosti, napadač može prepisati ključne fajlove sistema ili postaviti maliciozne fajlove, što može dovesti do daljinskog izvršavanja koda ili eskalacije privilegija. Problem je nastao zbog neadekvatnih provera u okviru funkcionalnosti modula mod_copy.

1.2 Opis eksploita

Izvor eksploita:

https://www.exploit-db.com/exploits/36803

Metod eksploatacije:

Eksploit koristi FTP komande SITE CPFR (copy from) i SITE CPTO (copy to), koje modul mod_copy pruža, kako bi kopirao zlonamerne fajlove na server. Napadač može postaviti PHP web shell u direktorijum koji je dostupan preko web servera, čime dobija mogućnost daljinskog izvršavanja komandi putem web interfejsa.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 Podešavanje eksploita

Ranljiv cilj: Eksploatacija je izvršena na metasploitable3 virtuelnoj mašini koja koristi ProFTPD sa omogućenom funkcionalnošću modula mod_copy. Verzija ProFTPD koja je pogođena ovom ranjivošću je 1.3.5 (ili ranije verzije). Servis radi na FTP portu 21, koji je poznat kao standardni port za FTP protokol.

Alati za eksploataciju: Korišćen je Metasploit alat za eksploataciju ranjivosti. Eksploit koji je odabran iz Metasploit baze nosi naziv: **proftpd_modcopy_exec**

2.2 Koraci eksploatacije

Prvo je potrebno pokrenuti Metasploit command prompt. Zatim unosimo komandu: **search cve-2015-3306** i dobijamo rezultat koji prikazuje dostupne exploite. Nakon toga biramo izvrsavanje exploita pomocu komande **use 0**. Nakon toga se pomoću komande info mogu pronaći dodatne informacije u vezi obaveznih i opcionih parametara samog eksploita. Neophodno je podesiti IP adresu ranjive mašine. To radimo komandom **set rhosts 10.1.1.112**

2.3 Rezultat eksploatacije

Nakon ovoga se pokrece i izvrsava exploit:

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

[*] Started reverse TCP handler on 192.168.56.1:4444

[*] 10.1.1.112:21 - 10.1.1.112:21 - Connected to FTP server

[*] 10.1.1.112:21 - 10.1.1.112:21 - Sending copy commands to FTP server

[*] 10.1.1.112:21 - Executing PHP payload /Uvm9Ml.php

[-] 10.1.1.112:21 - Exploit aborted due to failure: unknown: 10.1.1.112:21 - Failure executing payload

[] 10.1.1.112:21 - This exploit may require manual cleanup of '/var/www/html/Uvm9Ml.php' on the target

[*] 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 - ProFTPD: FTP session opened

Ovo pravilo generiše upozorenje kada se otvori FTP sesija na ProFTPD serveru. Praćenjem ovakvih sesija, SIEM alat pruža informacije o potencijalnim pokušajima neovlašćenog pristupa.

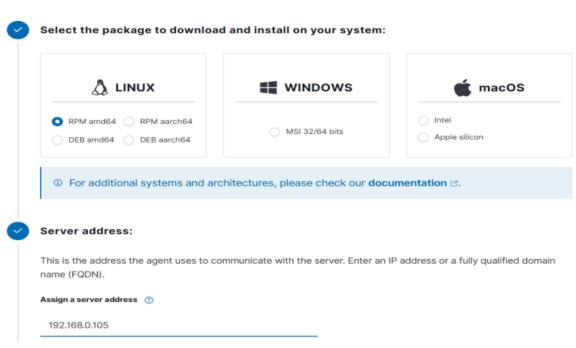
3.2 Konfiguracija SIEM-a

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

Deploy new agent



- 2. Unosimo IP adresu metasploitable3 virtuelne mašine
- U Metaploitable3 unosimo sledecu komandu: sudo nano /var/ossec/etc/ossec.conf l unosimo sledeće:

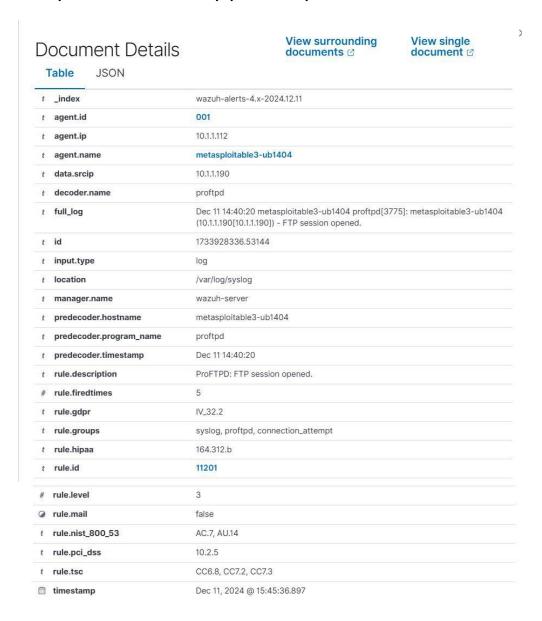
4. Unosimo komandu /var/ossec/bin/wazuh-control start

3.3 Proces detekcije

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



Takodje, mozemo videti i detaljnije informacije:



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)