

## Sniffing w sieciach z przełącznikami

# ETTERCAP-NG

Przedstawiamy narzędzie niezwykle upraszczające wykonanie ataków man in the middle.

JACEK SZUMOWSKI

### Wstęp

Ettercap-NG jest aplikacją stworzoną specjalnie do przeprowadzania sniffingu (węszenia) w sieciach z przełącznikami. W odróżnieniu od LAN-u opartego na koncentratorach, gdzie podsłuchiwanie ruchu jest bardzo proste, w sieciach ze switchami należy posłużyć się bardziej zaawansowanymi technikami. W większości wypadków praktyczne i samodzielne wykorzystanie tego typu metod (przeprowadzenie odpowiednich ataków) znane jest tylko doświadczonym administratorom. Ettercap-NG jest narzędziem, w którym odnajdziemy połączenie zaawansowanych technik dotyczących sniffingu i czytelnego interfejsu użytkownika. Należy jednak zauważyć, że do świadomego i pełnego wykorzystania możliwości programu konieczne będzie posiadanie odpowiedniej wiedzy.

Ettercap wydany jest na licencji GNU/GPL. Program dostępny jest dla następujących systemów operacyjnych: Linux, OpenBSD, FreeBSD, NetBSD, Windows, MacOS X, Solaris. Na potrzeby tego artykułu wykorzystana została wersja dla systemu Linux, działająca pod kontrolą dystrybucji Fedora Core 3.

### Możliwości programu

Ettercap-NG to pakiet, w którego skład wchodzi trzy współpracujące ze sobą programy: *ettercap* – sniffer dla sieci z przełącznikami, *etterlog* – analizator logów stworzonych przez ettercap oraz *etterfilter* – narzędzie do kompilowania plików źródłowych z filtrami. Sniffer, który jest najważniejszą częścią pakietu, posługuje się dwiema metodami. Pierwsza (domyślna) *UNIFIED* umożliwia sniffing wszystkich pakietów przepływają-

cych przez kabel sieciowy. Po zastosowaniu odpowiedniego ataku, ettercap modyfikuje pakiety w ten sposób, aby przepływały one przez nasz interfejs sieciowy. Druga metoda – *BRIDGET* – wykorzystuje dwa interfejsy sieciowe. Sniffujący komputer znajduje się pomiędzy komunikującymi się hostami.

Skuteczność programu gwarantuje użycie czterech typów ataku *man in the middle*. Pierwszy z nich (*arp*) polega na wysłaniu fałszywej ramki *arp reply* i zatruciu pamięci podręcznej *arp* atakowanego hosta. Drugi (*icmp*) rozsyła sfałszowane pakiety ICMP, wskazując ofierze „lepszą” drogę do Internetu. Kolejny (*dhcp*) polega na udawaniu przez atakującego serwera DHCP. Czwarta (*port*) technika polega na zalewaniu sieci LAN pakietami *arp*. Stosowana jest w wypadku, gdy *arp poisoning* (pierwsza metoda) jest nieskuteczna. Cel ataków jest wspólny. Wszystkie pakiety w sieci LAN mają być przekazywane przez komputer atakującego.

### Instalacja

Najnowszą wersję programu pobrać można z [1]. Po rozpakowaniu archiwum poleceniem `tar xzvf ettercap-NG-0.7.2.tar.gz` przechodzimy do katalogu z programem, wydając polecenie `cd ettercap-NG-0.7.2`. Instalacja z domyślnymi parametrami sprowadza się do wykonania kolejnych poleceń: `./configure`, `make` oraz z konta roota `make install`. Po zakończeniu programy *ettercap*, *etterfilter* i *etterlog* znajdują się w katalogu `/usr/local/bin`. W katalogu `/usr/local/etc` znaleźć można plik konfiguracyjny *etter.conf*, a wtyczki dla programu ettercap zainstalowane zostały w katalogu `/usr/local/lib/ettercap`. Użytkownik może mieć wpływ na dodatkowe parametry instalacji. Zostało to szczegółowo

opisane w pliku *INSTALL*, znajdującym się w katalogu z programem.

### Przykłady

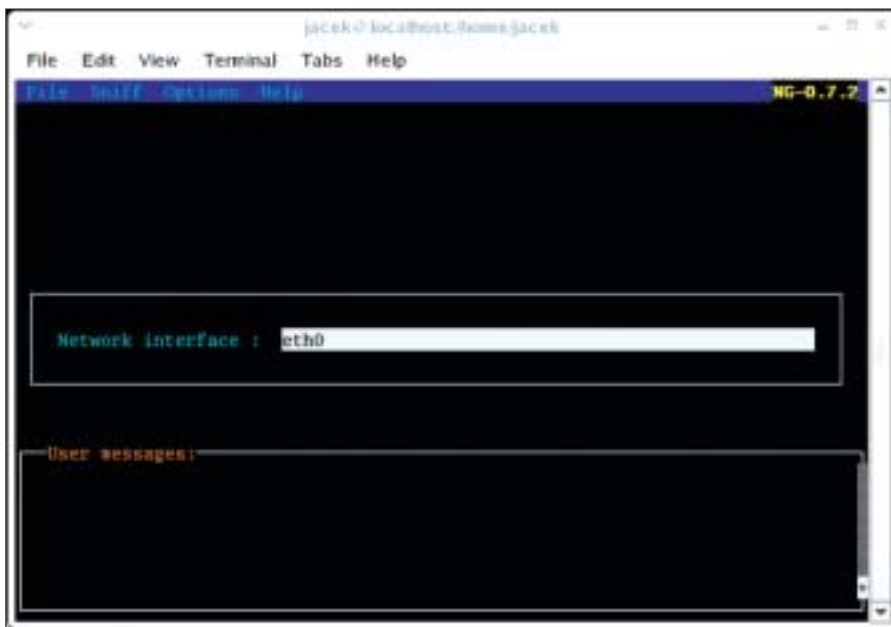
Pracując z programem *ettercap*, można korzystać z trzech rodzajów interfejsów. Polecenie *ettercap -G* korzysta z biblioteki *gtk* (Rysunek 1), a *ettercap -C* uruchomi program z interfejsem opartym na *ncurses* (Rysunek 2). Korzystanie z aplikacji pracującej w tych trybach



Rysunek 1: Ettercap wykorzystujący interfejs gtk.

nie powinno stwarzać problemów. Dlatego też w dalszej części opisane zostało wykorzystanie sniffera pracującego w konsoli tekstowej (Rysunek 3). Jednak informacje tam zawarte pomocne będą także dla użytkowników chcących wykorzystać interfejsy *ncurses/gtk*.

Przed przystąpieniem do wykonywania przykładów należy wspomnieć o możliwości konfiguracji programu przy pomocy edycji pliku *etter.conf*. Plik ten składa się z parametrów z domyślnie przypisanymi wartościami. Grupy ustawień zamknięte są w sekcjach: *[privs]* (określa z przywilejami jakiego użytkownika startuje program), *[mitm]* (szczegółowo



Rysunek 2: Ettercap wykorzystujący interfejs ncurses.



Rysunek 3: Ettercap wykorzystujący interfejs tekstowy.

we ustawienia parametrów dla dostępnych metod ataków), *[connections]* (parametry określające czasy połączeń), *[stats]* (ustawienia dotyczące statystyk), *[mis]* (np. ustawienia magazynu profili dla wykrytych hostów), *[dissectors]* (ustawienia portów dla dostępnych protokołów sieciowych), *[curses]* (dostosowuje kolory interfejsu ncurses do indywidualnych potrzeb), *[strings]* (np. ustawienia kodowania znaków). Rozpoczynając pracę z programem, warto jednak pozostawić większość parametrów domyślnych. Dopiero zdobyte później doświadczenie pozwolić może na świadomą modyfikację zaawansowanych ustawień zawartych w *etter.conf*.

Poniżej przedstawiono kilka przykładów umożliwiających podsłuchiwanie ruchu w sieci lokalnej:

```
ettercap -T -k /tmp/lista.txt /
```

powoduje utworzenie w katalogu */tmp* pliku *lista.txt* z listą hostów w sieci lokalnej.

Przy kolejnym uruchomieniu programu możemy wykorzystać wcześniej utworzony plik:

```
ettercap -T -j /tmp/lista.txt -M arp
```

To polecenie wykonuje atak *arp spoofing* na wszystkie hosty zawarte w */tmp/lista.txt*. Po wykonaniu tej komendy możliwe jest interaktywne wydawanie poleceń. Ich listę otrzymamy po wciśnięciu klawisza *h*. Klawisz *l* wyświetla listę podglądanych hostów, *c* pokaże wszystkie połączenia, a klawisz *o* powoduje rozwinięcie podmenu z opcjami, które umożliwiają uzyskanie szczegółowych informacji o sniffowanych hostach. Program opuścimy, naciskając klawisz *q*. Ettercap pozwala zawęzić pole poszukiwań do określonego portu czy hosta.

Poleceniem

```
ettercap -T -j /tmp/lista.txt -Z  
M arp // //80
```

uzyskać można informacje dotyczące wszystkich połączeń w sieci lokalnej na porcie 80. Następnym przykładem:

```
ettercap -t -j /tmp/lista.txt -Z  
M arp /192.168.1.10-30/110,25 -Z  
L /tmp/logettercap
```

zawęzi odbieranie pakietów tylko do komputerów o adresach IP 192.168.1.10 do 30, zbierając informacje tylko o protokołach POP3 i SMTP. Dodatkowo opcja *L* powoduje zapisanie wyników pracy programu w dwóch plikach *logettercap.eci* i *logettercap.ecp* w kata-

logu */tmp*. Pierwszy z nich zawiera dane dotyczące hostów w sniffowanej sieci, a drugi przechwyconych połączeń.

Do analizy logów wygenerowanych przez ettercap służy program *etterlog*. Użycie tego programu może ograniczyć się do prostego wydania komend: *etterlog /tmp/logettercap.eci* :*etterlog /tmp/logettercap.ecp*. Warto ograniczyć ilość danych wyrzucanych na ekran przez etterlog. Zwłaszcza w wypadku plików z rozszerzeniem *.ecp*, ilość informacji może być przytłaczająca. Oto kilka przykładów:

```
etterlog -k -l /tmp/etterlog.eci
```

wyświetli informację o hostach lokalnych w domyślnych kolorach,

```
etterlog -c /tmp/etterlog.ecp
```

wyświetli tablicę połączeń,

```
etterlog -t tcp //25 /tmp/  
etterlog.eci
```

wyświetli listę hostów z otwartym portem 25. Uruchamiając *etterlog* z opcją *-a*, otrzymać można statystyki dotyczące przeprowadzanego sniffowania.

## Podsumowanie

Pakiet Ettercap-NG to narzędzie o bardzo dużych możliwościach. Informacje zawarte w artykule pozwalają zapoznać się tylko z częścią jego opcji, umożliwiają jednak wykonanie skutecznego sniffingu w sieciach z przełącznikami (osobom chcącym poszerzyć swoją wiedzę na temat pakietu Ettercap-NG, polecić można dobrze przygotowane strony podręcznika systemowego). Prostota, z jaką można to zrobić, uczy niedoświadczonego użytkownika pewnej pokory i uświadamia niebezpieczeństwo przechwycenia poufnych informacji. Przekonać też może o zasadności użycia połączeń szyfrowanych. Uczciwy użytkownik musi jednak pamiętać, że nie wolno mu wykorzystywać tego typu programów w sposób, który naruszałby cudzą prywatność. ■

## AUTOR

Jacek Szumowski jest administratorem sieci Muzeum w Koszalinie

## INFO

[1] Strona domowa programu Ettercap-NG: <http://ettercap.sourceforge.net/>