Relazione progetto gestione di rete

DNS FILTER

Federico Germinario

Anno 2018/2019

1 Introduzione

DNS Filter consente di bloccare le richieste dns relativi a domini non ritenuti sicuri effettuate da un dispositivo di rete. I pacchetti dns vengono filtrati in base a 2 policy:

1. Policy impostata dall'utente (policy.txt) [1].
2. Siti web ritenuti non sicuri (blacklist-hostnames.txt)

Esempio di policy che blocca le richieste dns di unipi.it e facebook.com:

```
1 unipi.it
2 facebook.com
```

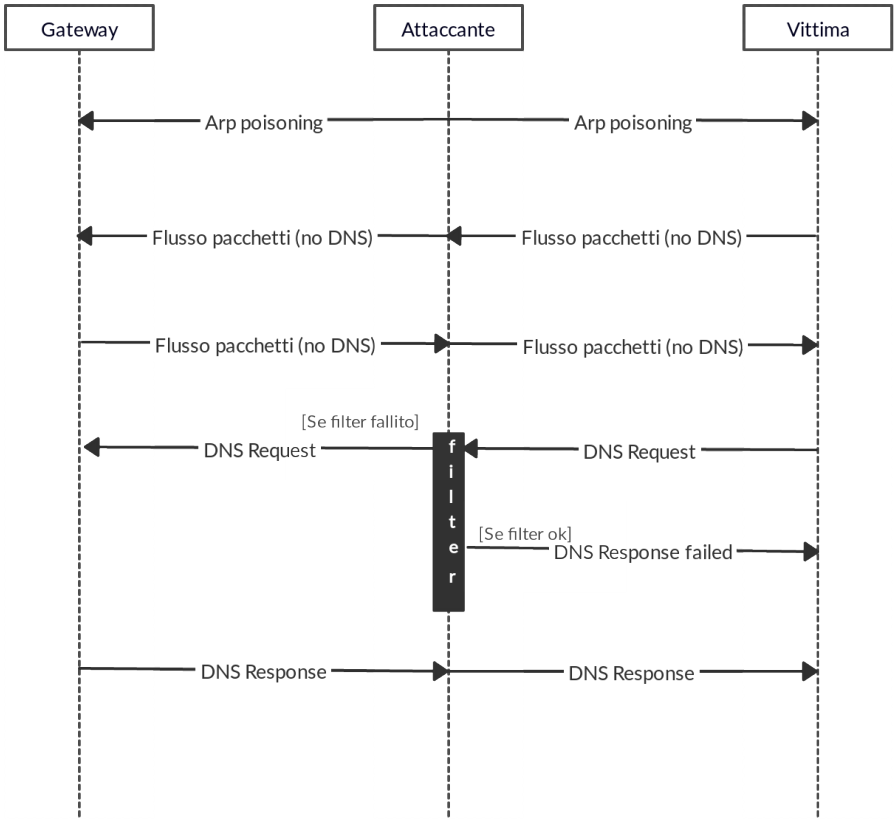
Il software utilizza la libreria Scapy che permette la manipolazione dei pacchetti di rete e consente di assemblare o decodificare i pacchetti di un ampio numero di protocolli, inviarli, catturarli, filtrare richieste e risposte.
Il software utilizza un attacco di tipo Man in the middle per intercettare le comunicazioni tra un dispositivo e il gateway. L'attacco prende il nome di ARP Spoofing poichè sfrutta una vulnerabilità dell'ARP (mancanza di autenticazione), inviando ARP Reply modificate per alterare la comunicazione.

2 Descrizione del software

Il software consente di sniffare i pacchetti dns e in base alle policy decide se inoltrarli oppure bloccarli mentre tutti gli altri pacchetti, vengono inoltrati automaticamente al gateway. Il tool sfrutta 4 thread. Il primo consente di effettuare l'Arp spoofing, inviando periodicamente pacchetti Arp Reply avvelenati alla macchina vittima e al gatawey. Il secondo permette di sniffare il traffico dns proveniente dalla macchina vittima, decidendo se forwardare il pacchetto al gateway oppure bloccarlo in base alle due policy descritte. Il terzo thread non fa altro che inoltrare i pacchetti verso il gateway.
Se un pacchetto viene filtrato e quindi non inoltrato al gateway, il software invierà una DNS Response non valida alla vittima. Questo stratagemma ci consente di non ricevere molteplici richieste dns uguali dalla macchina vittima, perchè se così non fosse, non avendo ricevuto risposta, continuerebbe ad inviare pacchetti DNS Request fino al raggiungimento del timeout.
Nel tool è presente anche un file di log che consente di tener traccia di tutti i pacchetti dns che sono stati filtrati.
Per memorizzare i domini che devono essere filtrati, ho utilizzato, per una maggiore efficienza del tool, 2 tabelle hash.

[1] Ciascuna riga del file costituisce un filtro

Il diagramma di sequenza sottostante mostra il fuzionamento generale del software:



3 Utilizzo

3.1 Esecuzione

Il tool deve essere eseguito da un utente con i privilegi di root.
Parametri da passare al software:

```
$ python dns_filter.py –help

  DNS FILTER
  optional arguments:
      -h, –help            show this help message and exit
      -i INTERFACE, –interface INTERFACE
                           network interface to attack on
      -r RANGE, –range RANGE
                           Local network scan range
```

3.2 Esempio di utlizzo

```
$ sudo python dns_filter.py -i enp2s0 -r 192.168.1.0./24
  [*] Initial setup
  [*] Reading file in progress...
  [*] Reading completed!

  [*] Interface: enp2s0
  [*] Range scan: 192.168.1.0/24
  [*] Gateway: 192.168.1.1 [74:da:da:c1:94:04]

  [*] Network scan in progress...
  Target: [0] - IP: 192.168.1.12 [68:9A:87:E5:16:0C]
  Target: [1] - IP: 192.168.1.10 [8A:CD:D2:34:7D:50]
  Target: [2] - IP: 192.168.1.14 [DC:4F:22:0F:2B:2E]
  Target: [3] - IP: 192.168.1.1 [74:DA:DA:C1:94:04]
  Selection Number: 1

  [*] Target: 192.168.1.10 [8A:CD:D2:34:7D:50]
  [*] Beginning the ARP poison
  [*] Beginning sniffing

  Forwarding: google.com
  Forwarding: github.com
  Request dns unipi.it dropped!
  Request dns facebook.com dropped!

  Keyboard Interrupt (CTRL+C)...Closing...
  [*] ARP Table restored to normal!
```

3.3 Dipendenze

- Nmap

```
$ pip install python-nmap
```

- Scapy

```
$ pip install scapy
```

4 Testing

Il tool è stato testato sul sistema operativo Ubuntu 19.04.
Per effettuare i test ho utilizzato come macchine vittime 2 sistemi operativi: Windows 10 e Ubuntu 19.04.
E' possibile utilizzare il software sia con collegamenti Ethernet sia Wireless.
Router utilizzato per il testing: D-Link AC750