Analisi del Traffico DNS con Wireshark

Il presente documento descrive dettagliatamente l'analisi del traffico **DNS** utilizzando **Wireshark**, con particolare attenzione alle query e alle risposte DNS. L'obiettivo è comprendere come i dispositivi comunicano con i server DNS per la risoluzione dei nomi di dominio e identificare eventuali vulnerabilità nel protocollo.

Requisiti:

* Un PC con **Wireshark** installato.
* Accesso a Internet.
* Permessi di amministratore per la cattura dei pacchetti di rete.

Procedura:

1. Cattura del Traffico DNS

Installazione di Wireshark:

Se non si dispone già di Wireshark installato:

* Scaricare l'ultima versione da Wireshark.org.
* Installare il software seguendo le istruzioni a schermo. **(Nota: non installare USBPcap se non necessario).**
* Avviare **Wireshark**.

Avvio della Cattura del Traffico:

* Selezionare un'interfaccia di rete attiva (es. Ethernet o Wi-Fi).
* **Svuotare la cache DNS** per evitare che i risultati siano già risolti:
  * Su **Windows**: aprire il prompt dei comandi e digitare: ipconfig /flushdns
  * Su **Linux** (dipende dal servizio in uso): sudo systemd-resolve —flush-caches
  * Su **macOS**: sudo killall -HUP mDNSResponder
* **Avviare la cattura** su Wireshark e visitare alcuni siti web per generare traffico DNS.

2. Analisi delle Query DNS

Filtraggio dei Pacchetti:

Dopo aver catturato il traffico, filtrare solo le richieste DNS:

udp.port == 53

Ciò consente di isolare solo il traffico DNS (che utilizza la porta 53 su UDP).
Interpretazione dei Pacchetti di Query

Un tipico pacchetto DNS di query include:

* **Transaction ID:** un identificatore univoco per la richiesta.
* **Flags:** campo che indica il tipo di richiesta.
* **Query Name:** il nome del dominio richiesto (es. www.google.com).
* **Query Type:** indica se è una richiesta **A** (IPv4) o **AAAA** (IPv6).

Analizzando i dettagli di una query in Wireshark, potremmo vedere:

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
```

```
Ethernet II, Src: 00:1a:2b:3c:4d:5e, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 49152, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x1234
    Flags: 0x0100 (Standard query)
    Queries: 1
    Query Name: www.google.com
    Query Type: A (Host Address)
```

Osservazioni

La richiesta proviene dall'indirizzo IP **192.168.1.10** e viene inviata al server DNS **8.8.8.8** (Google DNS). Viene effettuata una richiesta di tipo **A**, ovvero un indirizzo IPv4.

Analisi delle Risposte DNS

Filtraggio delle Risposte

Per isolare le risposte DNS, utilizziamo il filtro:

```
dns.flags.response == 1
```

Esempio di Risposta DNS

Ecco un esempio di risposta DNS a una query:

```
Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: 8.8.8.8, Dst: 192.168.1.10
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.10
User Datagram Protocol, Src Port: 53, Dst Port: 49152
Domain Name System (response)
    Transaction ID: 0x1234
    Flags: 0x8180 (Standard query response, No error)
    Questions: 1
```

```
Risposta RRs: 1
Richieste:
    Nome della richiesta: www.google.com
Risposte:
    Nome: www.google.com
    Tipo: A (Indirizzo host)
    Indirizzo: 142.250.184.100
```

Il server DNS **8.8.8.8** ha risposto fornendo l'indirizzo **142.250.184.100** per www.google.com.
Il campo Flags: 0x8180 indica che la richiesta è stata elaborata con successo.

L'analisi del traffico DNS con Wireshark è uno strumento potente per comprendere il funzionamento del protocollo, identificare anomalie e rilevare eventuali attacchi.