Progetto di Gestione di Reti

Andrea Tarabelli

July 22, 2018

Monitoraggio del traffico di rete di un dispositivo in LAN

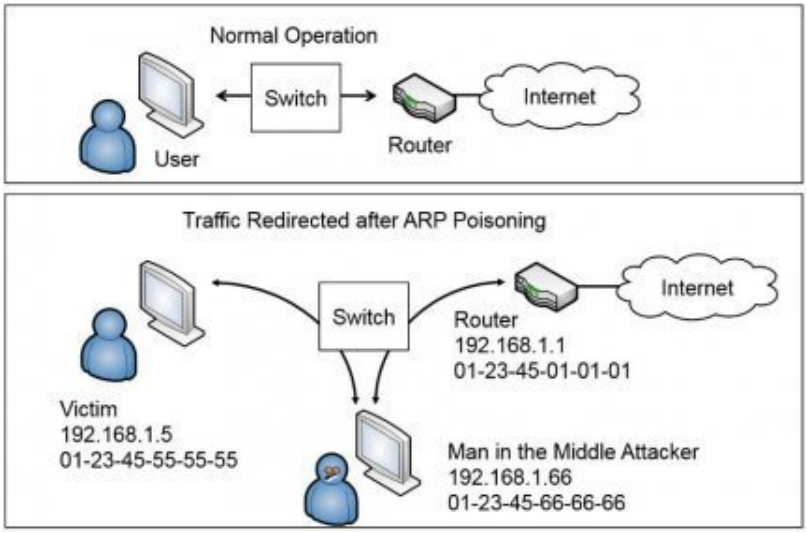
Contents

Abstract

NetworkMonitor è un programma per l'acquisizione e l'analisi del traffico internet di un dispositivo situato in una LAN, che utilizza tecniche di arp spoofing. Tale programma è in grado di mostrare le richieste DNS sul terminale e le analisi, ricavate dai pacchetti TCP e UDP, con un'interfaccia web offerta dallo strumento Chronograf.

1 Descrizione

Lo scopo del progetto è quello di rendere possibile l'analisi del traffico di rete di un host collegato ad una lan, senza l'utilizzo di strumentazione specifica e costosa, senza dover accedere al device monitorato. Il programma utilizza una debolezza del protocollo ARP: ovvero la mancanza di un meccanismo di autenticazione, rendendo così possibile l'intercettazione dei pacchetti di rete destinati ad altri device. Questa tecnica utilizza l'ARP poisoning che consente di attuare un attacco di tipo man in the middle, grazie ad opportune manipolazioni dei protocolli di livello 2. Il protocollo ARP ha la funzione di tradurre indirizzi IP in indirizzi di livello collegamento MAC. L'ARP poisoning consiste nell'inviare intenzionalmente risposte ARP(ARP reply), contenenti dati inesatti. In questo modo la tabella ARP (ARP cache) di un host conterrà dati alterati con lo scopo di ridirezionare il traffico verso la macchina dell'analista. Il programma che monitorando la rete riesce quindi a decodificare il contenuto dei pacchetti, e a compiere un'analisi. L'esigenza di praticare questo attacco è dovuta al fatto che ormai nelle recenti reti sono presenti gli switch, che grazie alla CAM table, permettono di inoltrare il traffico soltanto all'host di destinazione rendendo impossibile lo sniffing passivo. Le informazioni sul traffico vengono salvate in un database di serie temporali Influxdb che successivamente possono essere visualizzate su grafici costruiti con query l'applicazione Chronograf. Dopo aver concretizzato il MITM, l'analista sarà quindi in grado di sniffare, ovvero, leggere tutto il traffico da e per il target device.



Es: La cache ARP della vittima dovrebbe includere questa voce per inviare dati al router: 192.168.1.1, 01-23-45-01-01-01 .Tuttavia, dopo aver avvelenato la cache ARP, include questa voce: 192.168.1.1, 01-23-45-66-66-66. La vittima ora invia tutto il traffico, destinato al router, all'attaccante. L'analista acquisisce i dati per l'analisi, e utilizza l'inoltro IP per mantenere il traffico della rete regolare.

2 Installazione

Per l'installazione eseguire queste istruzioni

```
sudo apt install python3-influxdb
sudo apt install python3-pip
```

Se si preferisce usare un ambiente virtuale

```
sudo pip3 install virtualenv
virtualenv venv
source venv/bin/activate
```

Il programma ha molte dipendenze che devono essere installate con i comandi
Per i moduli python

```
sudo pip install -r requirements.txt
```

Per installare gli strumenti del database andare sul sito:

```
https://portal.influxdata.com/downloads
```

Per avviare i servizi:

```
service influxdb start
service chronograf start
```

Infine copiare il file chronograf-v1.db in /var/lib/chronograf/ per importare le impostazioni dashboard

NB: per il corretto funzionamento assicurarsi che la porta TCP di influxdb sia 8086.

3 Esecuzione

Per essere avviato correttamente è necessario inserire delle informazioni obbligatorie:

- L'interfaccia di rete, specificata dall'opzione -i.
- L'indirizzo IP del gateway, specificata dall'opzione -g.
- L'indirizzo IP del target, specificata dall'opzione -t.

```
Es: sudo python NetworkMonitor.py -i enp2s0 -t 192.168.1.3 -g 192.168.1.1
```

Successivamente accedere alla pagina web http://localhost:8888, selezionare la voce dashboard ed infine Network Monitor.

4 Implementazione

Il software è un'applicazione in linguaggio python versione 3 sviluppato per sistemi operativi linux e testato sulle distro basate su debian: linux mint 18.3 e ubuntu 18.04.

Sono state utilizzate principalmente due librerie:

1. ***scapy***: è uno strumento per la manipolazione e la decodifica dei pacchetti che fornisce un'interfaccia per la libreria in C libpcap, (WinPCap su Windows). Nel progetto è usato per la cattura e l'invio dei pacchetti.

2. ***influxdb***: è un client per l'interazione con InfluxDB un database distribuito di serie temporali, usato per la memorizzazione dei dati ricavati dall'analisi su un database.

Composto da 3 thread:

- POISON_THREAD: ha il compito di avvelenare le tabelle arp dell'host target e del gateway inviando delle arp reply falsificate, perchè hanno come MAC sorgente quello del host dell'analista e come IP quelli dei device da raggirare. Le risposte arp vengono inviate alla scadenza di un tempo casuale calcolato in base alle tempistiche di aggiornamento delle entry nelle arp cache.

- SNIFFER_THREAD: utilizza scapy per catturare i pacchetti sull'interfaccia di rete scelta dall'utente e filtrati per MAC del target. Mostra le query

DNS e allo scadere del timeout genera le statistiche di rete che invia come serie temporali al database.

- MAIN: recupera gli indirizzi MAC del target e del gateway, attiva i comandi per l'ip forwarding ed infine attende la richiesta di chiusura del programma.

4.1 Architettura