Laboratori giorno 3 – Cisco CyberOps

Relazione: Esplorazione del Traffico DNS

1. Introduzione

L'obiettivo di questo laboratorio è comprendere il funzionamento del protocollo DNS (Domain Name System) e analizzare il traffico DNS utilizzando lo strumento di cattura pacchetti Wireshark . Il DNS è un componente fondamentale delle reti informatiche, poiché traduce i nomi di dominio leggibili dagli umani (es. www.cisco.com) in indirizzi IP utilizzabili dai computer per comunicare. Durante il laboratorio, abbiamo catturato e analizzato il traffico DNS generato da query verso il dominio www.cisco.com, esaminando sia le query che le risposte DNS.

2. Metodologia

Per completare il laboratorio, sono stati seguiti i seguenti passaggi:

1. Installazione di Wireshark :
    - Installato Wireshark su Kali Linux utilizzando il comando:
    - sudo apt install wireshark -y
2. Cancellazione della Cache DNS :
    - Cancellata la cache DNS per assicurarsi che le query DNS fossero generate durante l'esperimento:
    - sudo systemd-resolve --flush-caches
3. Cattura del Traffico DNS :
    - Avviato Wireshark e selezionata l'interfaccia di rete attiva (eth0).
    - Generata una query DNS utilizzando il comando:
    - nslookup www.cisco.com
    - Catturato il traffico DNS risultante.
4. Analisi dei Pacchetti :
    - Filtrato il traffico DNS in Wireshark utilizzando il filtro:
    - udp.port == 53
    - Analizzati i pacchetti di query e risposta DNS.

3. Analisi dei Dati

3.1 Configurazione di Rete

- Indirizzo IP del PC : 192.168.1.59
- Subnet Mask : 255.255.255.0
- Indirizzo MAC del PC : 08:00:27:6e:13:6e
- Gateway Predefinito : 192.168.1.1
- Server DNS Configurato : 192.168.1.1

3.2 Query DNS

- Pacchetto DNS di Query :
    - Indirizzo IP Sorgente : 192.168.1.59 (PC locale)
    - Indirizzo IP Destinazione : 192.168.1.1 (server DNS/gateway)
    - Porta Sorgente : Porta dinamica (56831, 49375)
    - Porta Destinazione : 53 (porta standard per DNS)
    - Dettagli della Query :
        - Transaction ID : Identificatore univoco della transazione.
        - Flags : Flag "Recursion desired" impostato.
        - Queries :
            - Nome del dominio richiesto: www.cisco.com
            - Tipo di record richiesto: AAAA (indirizzo IPv6)

3.3 Risposta DNS

- Pacchetto DNS di Risposta :
    - Indirizzo IP Sorgente : 192.168.1.1 (server DNS/gateway)
    - Indirizzo IP Destinazione : 192.168.1.59 (PC locale)
    - Porta Sorgente : 53
    - Porta Destinazione : Porta dinamica (es. 56831, 49375)
    - Dettagli della Risposta :
        - Flags : Flag "Recursion available" impostato.
        - Answers :
            - Record AAAA:
                - 2a02:26f0:8d00:ca9::b33
                - 2a02:26f0:8d00:c9e::b33
        - Alias (CNAME) :
            - www.cisco.com ⟶ www.cisco.com.akadns.net
            - www.cisco.com.akadns.net ⟶ wwwds.cisco.com.edgekey.net
            - wwwds.cisco.com.edgekey.net ⟶ wwwds.cisco.com.edgekey.net.globalredir.akadns.net

- wwwds.cisco.com.edgekey.net.globalredir.akadns.net → e2867.dsc.a.akamaiedge.net

3.4 Confronto con nslookup

Eseguito il comando nslookup www.cisco.com:

Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsc.a.akamaiedge.net.
Name: e2867.dsc.a.akamaiedge.net
Address: 23.49.196.116
Name: e2867.dsc.a.akamaiedge.net
Address: 2a02:26f0:8d00:c9e::b33

- I risultati di nslookup corrispondono ai dati catturati in Wireshark, confermando la coerenza delle informazioni.

4. Riflessioni e Implicazioni di Sicurezza

4.1 Vulnerabilità del Traffico DNS

- Il traffico DNS in chiaro può essere intercettato da un attaccante sulla stessa rete, permettendo di:
  - Monitorare i siti web visitati.
  - Manipolare le risposte DNS per reindirizzare il traffico verso server malevoli.

4.2 Misure di Protezione

- Crittografia del Traffico DNS :
    - Implementare protocolli come DNS over HTTPS (DoH) o DNS over TLS (DoT) per crittografare il traffico DNS.
- Monitoraggio del Traffico :
    - Utilizzare strumenti come Wireshark per rilevare attività sospette, come query DNS verso domini malevoli.
- Configurazione del Server DNS :
    - Utilizzare server DNS affidabili e sicuri, come quelli forniti da Cloudflare (1.1.1.1) o Google (8.8.8.8).

5. Conclusioni

Questo laboratorio ha permesso di comprendere il funzionamento del protocollo DNS e di analizzare il traffico DNS utilizzando Wireshark. Abbiamo osservato come una query DNS viene risolta attraverso una serie di alias (CNAME) prima di raggiungere gli indirizzi IP finali. Inoltre, abbiamo evidenziato le vulnerabilità del traffico DNS in chiaro e discusso le misure di sicurezza necessarie per proteggere il traffico di rete.