Cisco CyberOps

Laboratorio - Esplorazione del Traffico DNS

In questo laboratorio, completa i seguenti obiettivi:

- Catturare il traffico DNS
- Esplorare il traffico delle query DNS
- Esplorare il traffico delle risposte DNS

https://itexamanswers.net/17-1-7-lab-exploring-dns-traffic-answers.html

Relazione

Durante il laboratorio, ho configurato la macchina virtuale con Windows 10 Pro in modo che la scheda di rete fosse impostata in modalità "bridge". Questa configurazione ha permesso alla macchina virtuale di utilizzare direttamente la rete fisica del mio computer, ottenendo un proprio indirizzo IP sulla stessa subnet del dispositivo host. Di seguito, descrivo i passaggi completi del laboratorio, includendo questa configurazione.
Ho avviato la macchina virtuale con Windows 10 Pro utilizzando il software di virtualizzazione installato sul mio sistema. Prima di iniziare, ho verificato le impostazioni della rete della macchina virtuale. All'interno del gestore della VM, ho selezionato la scheda di rete e l'ho configurata in modalità "bridge".

Questo ha permesso alla macchina virtuale di collegarsi direttamente alla rete locale del mio sistema, facilitando la comunicazione con i server DNS e simulando un ambiente di rete reale.
Dopo aver avviato la macchina virtuale, ho aperto Wireshark e selezionato l'interfaccia di rete associata alla macchina virtuale in modalità "bridge". Ho cliccato su "Start" per avviare la cattura del traffico. Subito dopo, ho aperto il browser Microsoft Edge (preinstallato sulla macchina virtuale) e ho visitato alcuni siti web, come example.com e wikipedia.org. Ogni accesso ha generato traffico DNS visibile in tempo reale su Wireshark.
Per analizzare il traffico DNS, ho applicato il filtro dns nella barra dei filtri di Wireshark. Grazie a questo filtro, ho isolato tutti i pacchetti pertinenti e ho potuto concentrarmi sull'analisi delle richieste e delle risposte DNS. Ho selezionato alcune richieste nel riquadro superiore e, nel riquadro inferiore, ho espanso la sezione "Domain Name System (query)" per visualizzare i dettagli. Ho osservato i domini richiesti, i tipi di record richiesti (come i record A) e le risposte fornite dai server DNS.
Un esempio interessante è stata la richiesta per un dominio che non era ancora stato risolto, che ha generato una query verso un server DNS upstream. Ho analizzato la risposta corrispondente, verificando l'indirizzo IP restituito e altri dettagli come il campo "Time To Live (TTL)", che indica il tempo durante il quale la risposta rimarrà valida nella cache DNS.
Al termine delle catture, ho salvato i dati in un file PCAP cliccando su "File" > "Save As" in Wireshark. Questo file può essere ricaricato successivamente per ulteriori analisi o esercizi. L'intero laboratorio è stato eseguito con successo, e l'utilizzo della modalità "bridge" per la rete della macchina virtuale ha garantito un'analisi realistica del traffico DNS. Grazie a questa configurazione, ho potuto lavorare in un ambiente isolato senza influire sul sistema host, comprendendo meglio il funzionamento del protocollo DNS.

Daniel_Gabriel_Costeanu