Verifica VE – Sistemi e Reti – 07/05/2024

Esercizio 1: Analisi del traffico ICMP

1. Apri un terminale e diventa utente privilegiato
   *(**trick**: "splitta" orizzontalmente/verticalmente Terminator, così da disporre di almeno un paio di tab/finestre appaiati/e).*
2. Installa il pacchetto software *tcpdump,* digitando il comando *apt-get install tcpdump.*
3. Digita il comando */sbin/ifconfig* e prendi nota del ***nome*** dell'interfaccia connessa alla rete locale.
4. Digita il comando *ip route show default* e prendi nota dell'***indirizzo IP*** del gateway (IP che appare dopo "*default via*")
5. In una finestra avvia *tcpdump*: *tcpdump -i nome-interfaccia icmp*
6. Nell'altra finestra avvia il comando *ping*: *ping -c 4 indirizzo-IP-gateway*
7. Commenta esaustivamente la comunicazione intercettata da *tcpdump*, supportando l'argomentazione mediante l'utilizzo di screenshot.
8. Avvia *Wireshark* e ripeti la stessa sessione di *ping* catturata precedentemente con *tcpdump*. Confronta e documenta le differenze nell'output di Wireshark rispetto a *tcpdump*. Focalizzati sui dettagli aggiuntivi che Wireshark potrebbe rivelare, come l'analisi grafica del flusso comunicativo e l'identificazione di altri protocolli coinvolti nel traffico.

Esercizio 2: Scansione di un host

1. Apri un terminale e assicurati di avere i privilegi necessari per installare software. Installa *nmap*, se non è già presente, con il comando: *apt-get install nmap*
2. Trova l'indirizzo IP del tuo gateway con il comando: *ip route show default (*nota l'indirizzo IP che appare dopo "default via").
3. Utilizza questo indirizzo per eseguire una scansione con nmap: *nmap -Pn IP-gateway*
4. Analizza l'output per identificare quali servizi sono esposti, specificando i protocolli e i relativi livelli della pila protocollare coinvolti. Rifletti su come queste informazioni possano essere utilizzate da un amministratore di rete o un analista di sicurezza per migliorare le misure di protezione della rete. Come, invece, queste stesse informazioni potrebbero essere utilizzate da un malintenzionato?

Esercizio 3: Wireshark e analisi del Three-way handshake

A partire da un protocollo dello strato applicativo a scelta (e quindi da una richiesta client generata all'interno di tale protocollo), intercetta ed analizza in Wireshark il processo di *three-way handshake,* anche identificando e commentando gli attributi più significativi, supportando la tua trattazione con screenshot.

Consegna: produci un unico documento di testo contenente tutte le risposte agli esercizi. Rinomina il file in *Cognome-Nome.estensione* ed invialo al docente mediante: *http://consegna.byteriot.it*