Simulazione verifica di laboratorio – Marzo 2024 – VE

Esercizio 1: scenario progettuale (2 pt)
Scenario: la rete scolastica sta sperimentando un traffico broadcast eccessivo che degrada le prestazioni della rete. La rete attuale utilizza una singola subnet /16 per tutti i dispositivi (rintracciabile osservando l'output del comando *ifconfig* da terminale Linux).

- Discuti le potenziali cause dell'eccessivo traffico broadcast, non tralasciando un breve inciso sul tema "dominio di broadcast di livello 2 e 3".
- Proponi soluzioni, fornendo un esempio di come si potrebbe riconfigurare la rete, inclusi i nuovi range di indirizzi IP e l'eventuale configurazione delle VLAN, considerando che si desideri segmentare la rete attuale in 4 diverse aree: 3 laboratori e la segreteria.

Esercizio 2: analisi processo di rete (2 pt)
Si presuppone che il Web Server Apache sia stato correttamente installato sul proprio sistema (*apt-get install apache2*).

- Utilizza i comandi appropriati per determinare se l'applicazione è in esecuzione sul sistema (ad esempio: comandi da terminale per verificare lo stato dei processi, etc).
- Dimostra, inoltre, che sia correttamente in ascolto sull'interfaccia di *loopback*, pronta ad evadere richieste HTTP (ad esempio: comandi da terminale per l'analisi delle connessioni di rete, analisi del traffico/interazione HTTP con Wireshark, etc).

Documenta e commenta entrambe le operazioni, anche mediante l'ausilio di screenshot.

Esercizio 3: ICMP in broadcast (2 pt)
Da terminale, esegui un ping in broadcast all'indirizzo di broadcast della propria rete locale. Analizza con Wireshark in traffico di rete prodotto concentrandosi, in particolare, sugli attributi fondamentali dei vari PDU (IP src, IP dst, MAC src, MAC dst, etc).

PLUS. Prendi nota di quali dispositivi hanno prodotto una risposta (*echo response*) ed analizzane alcuni mediante l'applicativo *nmap* (*apt-get install nmap*). È possibile giungere alla conclusione che sistemi operativi diversi si comportino diversamente rispetto all'evasione di richieste pervenute in broadcast?

Esercizio 4: Analisi del traffico DNS (2 pt)
1. Da terminale digita il comando *cat /etc/resolv.conf* e prendi nota dell'indirizzo IP del proprio server DNS.
2. Apri Wireshark, ponendosi in ascolto sull'interfaccia opportuna.
3. Impostare il seguente filtro: *(tcp.port == 53 || udp.port == 53) && ip.addr == **IP DNS*** (dove ***IP DNS*** corrisponde all'indirizzo di cui al precedente punto 1).
4. Da terminale, digita il comando *host consegna.byteriot.it*
5. Commenta esaustivamente la comunicazione client-server intercettata da Wireshark, facendo emergere chiaramente le principali specifiche dei vari PDU nei diversi layer coinvolti, anche con l'ausilio di screenshot significativi.

Esercizio 5: Wireshark e analisi del Three-way handshake (2 pt)
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.

Consegna: produrre un unico file di testo (in formato DOC, DOCX, ODT), convertirlo in formato PDF. Rinominare il file in *Cognome-Nome.pdf* ed invialo al docente via Google Classroom.