Rețele de calculatoare

Lucrare de laborator nr. 3

Analiza pachetelor în simularea Cisco și în condiții reale Wireshark

Sarcini:

- Instalați programul pentru analiza traficului Wireshark și familiarizați-vă cu interfața
- Construirea topologiei rețelei în simulatorul Cisco Packet Tracer utilizând un analizor de rețea
- Studierea conținutului pachetelor de protocoale ICMP, ARP și STP în simulatorul Cisco
- Studierea pachetelor în analizorul de rețea Wireshark pe baza unor exemple reale.

Mod de lucru:

- Instalați simulatorul Cisco Packet Tracer și analizorul de rețea Wireshark
- Construiți o topologie simplă în simulator utilizând analizorul de rețea încorporat
- Trimiteți mai multe pachete prin topologie pentru a crea o înregistrare în analizorul de rețea
- Analizați pachetele care trec prin rețeaua de protocoale ICMP și ARP, făcând înregistrări.
- Familiarizați-vă cu interfața programului Wireshark.
- Cu analizatorul activat, accesați linkul furnizat și completați datele fictive în câmpurile de autentificare și parolă.
- Analizați cererea HTTP pentru a detecta prezența datelor neprotejate.
- De asemenea, cu analizatorul de trafic de rețea activat, completați date fictive pe pagina care are mențiunea HTTPS la începutul linkului.
- Folosind utilitarul ping, trimiteți mai multe pachete la adresa 8.8.8.8 pentru analiza protocolului ICMP.
- Folosind linia de comandă, ștergeți înregistrările ARP din tabel.
- Faceți o concluzie cu privire la munca depusă.

Conținutul raportului:

- Pagina de titlu
- Sarcini de îndeplinit
- Rezultatele lucrării, cu comentarii, imagini și explicații
- Concluzii privind munca depusă

Introducere

Analiza traficului de rețea este una dintre sarcinile cheie în domeniul rețelelor de calculatoare. Înțelegerea structurii pachetelor de rețea, a principiilor de transmitere a acestora și a interacțiunii protocoalelor de rețea permite diagnosticarea eficientă a defecțiunilor, identificarea vulnerabilităților și optimizarea funcționării rețelei. În condițiile creșterii volumului de date transmise și a complexității infrastructurii de rețea, abilitățile de analiză a traficului devin deosebit de relevante.

În această lucrare practică se utilizează programele Cisco Packet Tracer și Wireshark. Cisco Packet Tracer este un simulator de echipamente de rețea care permite simularea funcționării rețelelor locale și globale, configurarea routerelor, comutatoarelor și dispozitivelor finale, precum și urmărirea procesului de transfer de date între acestea. Utilizarea modului de simulare oferă posibilitatea de a observa vizual trecerea pachetelor prin rețea și de a analiza funcționarea diferitelor protocoale.

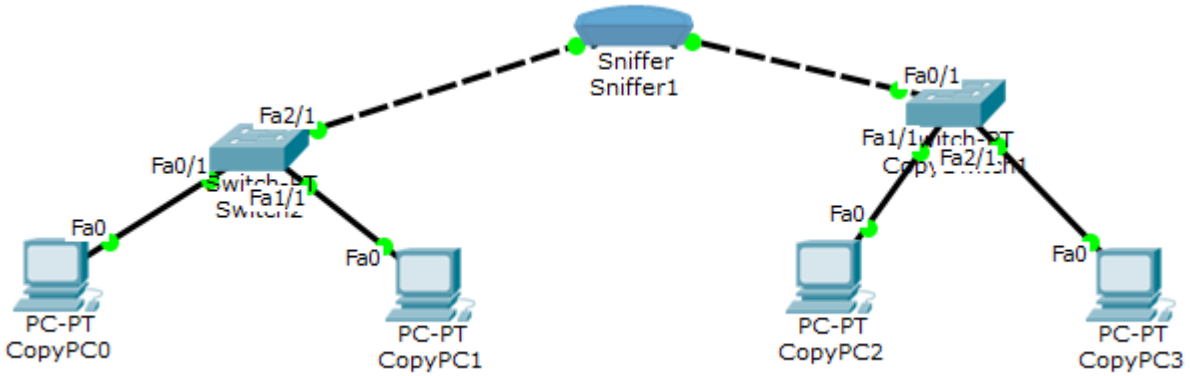
Wireshark este un analizator puternic de protocoale de rețea, destinat interceptării și studierii detaliate a traficului de rețea în timp real. Programul permite examinarea conținutului pachetelor la diferite niveluri ale modelului OSI, analizarea anteturilor protocoalelor, determinarea tipurilor de date transmise și identificarea posibilelor anomalii.

Scopul acestei lucrări este studierea structurii pachetelor de rețea, analiza trecerii lor prin rețea și consolidarea cunoștințelor teoretice despre funcționarea protocoalelor ICMP, ARP și HTTP în practică. În cursul lucrării, se planifică modelarea rețelei în Cisco Packet Tracer, generarea traficului de rețea și analiza acestuia cu ajutorul componentei integrate a simulatorului sniffer. Cu ajutorul Wireshark, se va analiza traficul în timp real.

Sarcini de realizat

Prima parte 1. Analiza pachetelor în simulatorul Cisco Packet Tracer.

În această parte, este necesar să se efectueze analize ale pachetelor care trec utilizând componentele integrate ale simulatorului de rețea Cisco Packet Tracer. Pentru analiza pachetelor se va utiliza snifferul integrat, este necesar să se construiască topologia rețelei conform schemei indicate, să se trimită mai multe pachete prin analizorul de rețea și să se analizeze conținutul acestora pe baza înregistrărilor salvate. Este necesar să se analizeze conținutul pachetelor de protocoale ICMP, ARP.



Schema 1. Topologie cu utilizarea snifferului.

Pași principali:

1. Construiți topologia rețelei conform schemei prezentate. Pentru construirea rețelei, utilizați 2 x Switch-PT (Generic), 4 x Computere, 1 x Sniffer (Categoria End devices).

2. Pentru conectarea la Sniffer, utilizați un cablu Copper Cross-Over.

3. Alocați adresele IP utilizând rețeaua 192.168.X.0 (X – numărul din grup) și masca 255.255.255.0.

4. Accesați interfața Sniffer, secțiunea GUI, și vizualizați lista inițială.

5. După distribuirea adreselor IP, trimiteți un pachet de tip ICMP (Simple PDU) de la PC 1 la PC 3.

6. Accesați interfața Sniffer și verificați ce pachete au fost transmise în rețea.

   Ce pachete au apărut după trimiterea unui singur pachet ICMP? Care sunt

adresele destinatarului și expeditorului? Care este indicatorul TTL (Time to Live)?

7. Analizați conținutul pachetelor ARP și ICMP.

   De ce se utilizează protocoalele ARP și ICMP în rețea? Câtă informație transmite fiecare? Ce reprezintă Ethernet Frame? La ce niveluri ale modelului OSI funcționează aceste protocoale?

Partea a doua 2. Analiza pachetelor în timp real folosind Wireshark.

În această parte, este necesar să se efectueze o analiză a pachetelor care trec prin rețea în timp real folosind analizorul de rețea Wireshark. Pentru a efectua analiza pachetelor, este necesar să se instaleze analizorul de rețea și să se aplice filtre pentru a obține rezultatele necesare.

1. Instalați analizatorul de rețea Wireshark.
2. În interfața deschisă a programului, instalați filtrul de rețea pe interfața „Rețea wireless”.
3. În linia de sus, puteți utiliza filtre pentru a identifica pachetele de protocoale necesare.
4. Cu analizatorul de pachete activat și filtrul „icmp” setat, accesați linia de comandă (CMD) și, utilizând utilitarul ping, trimiteți mai multe pachete de tip ICMP la adresa 8.8.8.8.
5. Verificați ce afișează analizatorul de rețea.

   Pachetele diferă de cele din simulator? Ce informații conțin pachetele protocolului ICMP?

6. Pentru a verifica funcționarea protocolului ARP, va trebui să ștergeți tabelul de înregistrări ARP. Porniți linia de comandă în numele administratorului.
7. Utilizați comanda „arp -a”. Ce rezultat ați obținut?
8. Fără a opri analizatorul de rețea. Introduceți comanda „netsh interface IP delete arpcache” pentru a șterge tabelul.

9. În analizorul de rețea, aplicați filtrul de rețea „arp”.

   Ce a rezultat în urma acțiunilor dvs.? Analizați rezultatul funcționării analizorului de rețea și pachetele ARP.

10. Porniți Wireshark, deschideți browserul web și conectați-vă la un server http neprotejat (de exemplu, http://www.vbsca.ca/login/login.asp) , introduceți informațiile de pe ecranul de autentificare (nume și parolă fictive) și trimiteți-le la server.

11. Opriți capturarea și analizați conținutul pachetelor, aplicând filtre de afișare.

12. Găsiți în capturile de pachete informațiile introduse pentru conectare.

    Care este adresa IP a dvs. și a serverului? Care este adresa MAC a dvs. și a serverului?

13. Efectuați aceleași acțiuni, dar utilizând un site cu certificat de securitate (HTTPS).

    Care este diferența între HTTPS și HTTP? De ce unele date nu sunt vizibile?