7 Зертханалық жұмыс №7. Қарапайым желілік конфигурацияны құру. IP-адрестеу. Желі мониторингі. Трафикті талдау. Желілік пакеттердіталдау үшін снифферлерді пайдалану

Жұмыстың мақсаты: желілік трафикті талдау принциптерін білу.

7.1 Әдістемелік нұсқаулар

1990 ж. басында хакерлермен пайдаланушылық логиндер мен парольдерді тәркілеу үшін кең қолданылды. Хабтардың кең таралуы үлкен сегментті желілерде ешқандай күшсіз трафикті тәркілеуге мүмкіндік берді.

Снифферлер жағымды да, сондай-ақ деструктивті желілерді де қолданады. Сниффер арқылы өтетін трафикті талдау:

1) Қосымшаның желілік белсенділігін қадағалауға.
2) Желілік қосымшалар хаттамаларын баптауға.
3) Конфигурация қателігі немесе дұрыс еместігін локальдау.
4) Паразитті, вирусты және сақиналанған трафикті табу, оның бар болуы желілік құрылғы мен байланыс арнасына жүктемені ұлғайтады.
5) Желіде зиянды және рұқсатсыз бағдарламалық қамтамаларды табу, мысалы, желілік сканерлер, флудерлер, трояндық бағдарламалар, пирингтік желі клиенттері және басқаралы.
6) Парольді және басқа ақпаратты табу мақсатымен кез келген шифрленбеген (кейде шифрленген де) пайдаланушылық трафикті ұстап алуға мүмкіндік береді.

7.2 Жұмысты орындауға тапсырмалар

1. Wireshark бағдарламасының интерфейсін меңгеру (\\corp.mgkit.ru\dfs\work\wireshark).
2. 100 дербес пакеттерді ұстап алу. Статистикалық деректерді анықтау:
- желідегі әртүрлі хаттамалар трафигінің пайыздық қатынасы;
- кадр/сек орташа жылдамдығы;
- байт/сек орташа жылдамдығы;
- пакеттің минималды, максималды және орташа өлшемі;
- каналды өткізу жолағын пайдалану дәрежесі (желі жүктемесі).
3. 20 IP-пакетті тіркеу. Статистикалық деректерді анықтау:
- Желіде tcp/ip стегінің әртүрлі хаттамалар трафигінің пайыздық хаттамасы;
- пакеттің минималды, максималды және орташа өлшемі.
4. Әдістемелік нұсқаулардан мысал бойынша ARP-хаттамасының талдауын орындау.
5. Кез келген IP-пакет мысалында Ethernet және IP хаттамаларының құрылымын көрсету. Тақырып өрістерін белгілеп, оларды сипаттау керек.

Ping утилитінің жұмыс істеу принципін талдау және сипаттама беру.

Утилитамен қолданылатын барлық хаттамаларды сипаттау керек. Хаттамалардың барлық өрістерін сипаттау. Ping утилитінің жұмыс істеуі кезінде машиналардың өзара әрекетінің диаграммасын құру.

Бақылау сұрақтары

1. Желілік трафик мониторингісінің негізгі мақсаттары қандай?
2. Трафик мониторингі фильтрациядан айырмашылығы неде?
3. Бағдарлама-сниффер класының міндеттері қандай?
4. Сниффердер қандай негізгі функцияларды орындайды?
5. Wireshark снифферін көрсету фильтрі мен тәркілеу фильтрі не үшін қолданылады? Олардың айырмашылығы неде?
6. Wiresharkснифферi тәркіленген пакеттерді статистикалық өңдеудің қандай базалық функцияларына ие?
7. ARP хаттамасы қандай есептерді шешуге арналған?
8. ARP хаттамасының қызметі қандай?