Практикалық жұмыс №7

Тақырыбы: Қарапайым желілік конфигурацияны құру. IP-адрестеу. Желі мониторингі. Трафикті талдау. Желілік пакеттерді талдау үшін снифферлерді пайдалану.

Мақсаты: Желілік пакеттерді талдау үшін снифферлерді пайдалану

Желідегі жұмыста қауіпсіздікті қамтамасыз ету

ДК ақпаратына рұқсатсыз кіру - онымен жасырын танысуды, өңдеуді, көшіруді, әр түрлі вирустарды,оның ішінде, бүлдіруші бағдарламалық өнімдерді, сондай-ақ ақпаратқа шығудың белгіленген ережелеріне қайшы келетін ақпарат өзгертуді немесе оны жоюды айтамыз.

ДК қорғау үшін сақталған ақпарат қауіпсіздігін қамтамасыз ету мүмкіндігін кеңітетін әр түрлі бағдарламалық әдістер қолданылады. Стандартты дербес компьютерді қорғау құралдарының ішінде кең таралғандары:

1. Парольдік ұқсастыруды (идентификацияны) пайдаланып, мүмкіндік ресурстарын қорғау құралдары.
2. Әр түрлі ақпаратты шифрлау әдістерін қолдану.
3. Компьютерлік вирустардан қорғау және архив құру

Ақпараттық қауіпсіздік жүйесін қарастырғанда әдетте екі мәселелер тобына бөледі: компьютер қаупсіздігі және желілік қауіпсіздік. Компьютердің қауіпсіздігіне деректерді қорғаудың барлық мәселелері жатады, яғни компьютерде сақталатын, өңделетін автономды жүйе ретінде қарастырылатын деректер мәселелері. Бұл мәселелер деректер қорымен, компьютердің енгізілген аппаратты құрылғыларымен, операциялық жүйе құралдарымен шешіледі. Желілік қауіпсіздік түсінігі желілік құрылғылар арасындағы ақпарат алмасу кезіндегі қорғау және рұқсатсыз енуден қорғау мәселелері болып табылады. Бірақ қазіргі уақытта компьютер мен желілік қауіпсіздікті бір-бірінен айырмашылығын анықтау өте қиын мәселе, олар бір - бірімен өте тығыз байланыста жатады. Тек желілік қауіпсіздік өзінің мамандығын қажет етеді. Жеке дара жағдайда жұмыс істеп тұрған компьютерге ішкі қол салудан сақтау үшін әртүрлі тиімді әдістерді қолдануға болады: мысалы клавиатураны құлыпқа жабу немесе қатты дискіні шығарып алып сейфке салып тастау. Желіде жұмыс істеп тұрған компьютер қоғамнан бөлініп қала алмайды ол басқа компьютерлермен кез-келген уақытта байланыста болуы керек. Сондықтан желіде қауіпсіздік қорғау өте күрделі жағдай болып есептеледі. Басқа қолданушының желіде жұмыс істеп тұрған компьютерді қолдануы логикалық тұрғыдан болуы шарт. Осындай жағдайда қауіпсіздікті қорғауды қамтамасыз ету бір ойға әкеліп соқтырады – яғни әрбір қолданушы үшін өзінің ақпаратты қолданатын құқығы желідегі әрбір компьютер үшін желілік байланыстарын реттеп отыру қажет. Бұл мәселелерден басқа желілер өзінің табиғатында тағы да бір қауіп түріне кездеседі. Желімен берілген хабарды ұстап қалу, анализдеу, «жалған» трафиктер құру. Желі қауіпсіздігін қорғаудың негізгі бөлшегі осы қылмыстың алдын алуға жұмсалады. Желілік қауіпсіздігінің мәселелері

корпоративті желілерден бөлінген каналдарға өту барысында көптеп байқалады. (Интернет, frame relay). Жалпы желіні қамтамсыз етушілер қазірше берілгендерді өзінің магистралы бойынша тасымалдау кезінде қолданушы деректерін қорғауды сирек қолданады. Бұл мәселені көбінесе құпиялылығын, бүтіндігін, ену мүмкіндігін қолданушының өзінің қамқорына қалдырады. Құпиялылықтың негізгі түсінігі деректердің бүтіндігі және ену мүмкіндігі. Қауіпсіз ақпараттық жүйе – ол біріншіден рұқсат етілмеген енуден қорғайды, екіншіден ақпаратты өзінің қолданушыларына барлық уақытта деректерге енгізе алады, үшіншіден ақпаратты сенімді сақтайды және деректердің өзгермеуін қамтамасыз ететін жүйе. Осылайша, анықтама бойынша қауіпсіз жүйе құпиялық, ену мүмкіндігімен, бүтіндік қасиетімен анықталады.

Құпиялылық (confidentiality) — бұл құпия деректерге ену тек қана рұқсат берілген қолданушыларға берілетіндігінің кепілі. (Бұл қолданушылар авторластырылған деп аталады).

Ену мүмкіндігі (availability) — авторластырылған қолданушылар барлық уақытта деректерге ену құқығы бар болуының кепілі.

Бүтіндігі (integrity) — деректерді түрлі жолдармен өзгертуге авторластырылмағандар үшін рұқсат етілмеуді қамтамасыз ететін дұрыс мәнді деректерді сақтаудың кепілі.

Нақты IP-адресі бар Интернет желісіне қосылу кезінде қорғауды қамтамасыз ету үшін әдетте маршрутизаторларға IP-сүзгілер орнатылады. Олардың қызметі ішкі желіге мәліметтерді нақты белгіленген компьютерге және нақты белгіленген протокол бойынша жеткізу.

1-тапсырма

TCP/IP желі терминологиясында желі маскасы деп желінің IP-адрес түйінінің қай бөлігі желі адресіне, ал қай бөлігі – осы желідегі тұйіннің адресіне жататынын көрсететін екілік санды айтады. Желінің белгіленген IP-адресі мен маскасына қарай желінің адресін табыңыз.

IP-адрес: 145.92.137.88 Маска: 255.255.240.0

Жауапты жазар кезде кестеде келтірілген IP-адрестің 4 элементін таңдаңыз және қажет ретпен сәйкес сандарды нүктесіз жазыңыз.

A
B
C
D
E
F
G
H
0
145
255
137
128

240
88
92

Жауабы: **BHEA**

Шығарылуы:
IP-адрес пен масканы екілік жүйеге ауыстырып, бір-біріне көбейтеміз.

IP-адрес: 145.92.137.88 10010001.01011100.10001001.01011000
Маска: 255.255.240.0 11111111.11111111.11110000.00000000
10010001.01011100.10000000.00000000

Шыққан санды ондық жүйеге ауыстырамыз, 145.92.128.0 (бұл желі адресі). Кесте бойынша оларға сәйкес келетін элементтерді нүктесіз жазып шығамыз, яғни BHEA.

2-тапсырма

Егер желі маскасы 255.255.252.0 және компьютердің желідегі IP-адресі 226.185.90.162, онда желідегі компьютердің реттік номері _____тең?

Жауабы: 674

Шығарылуы:
1. Желі маскасындағы екі октет (октет – 8 биттен тұратын масканың саны) 255-ке тең болғандықтан, екілік жүйеге ауыстырғанда 24 бірлік болып жазылады, демек алғашқы екі октет желі адресін анықтайды.
2. Желі маскасындағы 252 және 0 сандарын екілік жүйеге ауыстырамыз.
$252_{10}=11111100_2$,
$0_{10}= 00000000_2$.
3. IP-адрестің соңғы екі октетін екілік жүйеге ауыстырамыз.
$90_{10} =01011010_2$
$162_{10} =10100010_2$
4. Желідегі компьютердің маска мен адрестің екі соңғы октеттерін жазып шығамыз:
11111**00 00000000**
01011**0 10100010**
10 10100010
Қою түспен бізге керек сан белгіленген 0 санынан басталатын бөлікті астыңғы санға қосамыз, яғни $1010100010_2=674_{10}$

3-тапсырма

Кейбір ішкіжелілерге 255.255.248.0. маскасы қолданылады. Бұл маскаға компьютердің неше адресі қолданылады? *Ескерту:* Практикада компьютерді адрестеу үшін екі адрес қолданылмайды: желі адресі мен кеңарналы адрес.

Жауабы: 2046

Шығарылуы:
1. Маскадағы екі октет 255-ке тең, олар желінің адресі. Екілік жүйеге аударғанда 16 бірлік болады.
2. $248_{10}= 11111000_2$. Соңында 3 ноль, тағы 8 ноль масканың соңғы октетінен аламыз. Сонымен, 3+8=11 ноль компьютердің адресі болады.

3. 2^{11}=2048, екі адрес қолданылмағандықтан, 2048-2=2046

4-тапсырма

Қылмыс болған жерде 4 бөлік қағаз табылды. Тексеріс бойынша IP-адрестің фрагменттері екені белгілі болды. Тексерушілер бұл бөліктерді А, Ә, Б және В деп әріптермен белгілеген. IP-адресті қалпына келтіріңіз.

Жауабы: БӘВА

.64
2.16
16
8.32
А
Ә
Б
В

Шығарылуы:

IP-адрес 4 байттан тұрады. Әр байт 255-тен аспайды.
А бөлігіу бірінші орынға қоя алмаймыз, себебі адрес нүктеден басталмайды. В бөлігінен кейін Ә бөлігін қоя алмаймыз, себебі 255-тен аспау керек. Демек Ә бөлігін Б бөлігінен кейін қоямыз. А бөлігінен кейін В бөлігін қоя алмаймыз, себебі 255-тен аспау керек. Сонымен [16] [2.16] [8.32] [.64] 162.168.32.64, яғни БӘВА.

5-тапсырма

test.edu серверінде HTTP хаттама бойынша кіруге болатын demo.net файл орналасқан. Берілген файлдың адресінің фрагменттері А, Б ... Ж әріптерімен кодталған (кестені қараңыз). Берілген файлдың интернеттегі адресін кодтайтын әріптердің тізбегін жазыңыз.

А
test
Б
demo
В
://
Г
/
Д
http
Е
.edu
Ж
.net

Жауабы**: ДВАЕГБЖ**

Бақылау сұрақтары:

1. IP-адрестерінің қандай типтері мен кластарын білесіз?

2. Маршрутизация хаттамаларының маршруттық хаттамалардан айырмашылығы қандай?
3. Арақашықтық-векторлық маршрутизация мен каналдар жағдайының маршрутизациясы неге жауап береді?
4. Маршрутизацияның қандай әдістерін білесіз?
5. Айқын маршрутизация нені білдіреді?