Зертханалық жұмыс 2
Жергілікті трафикке талдау жүргізу үшін Network Monitor утилиті

Мақсаты: Жергілікті трафикке талдау жүргізу үшін Network Monitor утилитін қолдану. SNMP агенті және желіні басқару бағдарламасы арасында ақпарат алмасу мен мониторинг жүргізуді зерделеу. IPSec саясаттары мен ережелерін зерделеу. IPSec-ті баптау. Ережелер мен саясаттың көмегімен желіні қорғауды баптау. IPSec басқару және қателіктерді болдырмауды сипаттау.

Тапсырма 1:

1. Network Monitor утилитімен танысу.
2. Network Monitor-ды қолдану.
3. Қосылуды даярлау.
4. Терминалдар серверімен қатынауға мүмкіндік жасау.

Тапсырмасы бойынша компьютерде орындау:

Network Monitor-ды орнатыңыз

1. Start\Settings\Control Panel (Пуск\Настройка\Панель управления) (Қосу/Баптау/Басқару тақташасы) мәзірін ашыңыз және Add/Remove Programs (Установка и удаление программ) (Бағдарламаларды орнату және жою) жарлығын шертіңіз.
2. Add/Remove Windows Components (Добавление и удаление компонентов Windows) (Қосу және Windows компонеттерін жою) батырмасын шертіңіз.
3. Windows компоненттер шебері терезесінде Management And Monitoring Tools (Средства управления и наблюдения) (Басқару және бақылау құралын) таңдаңыз және Details (Состав) батырмасын шертіңіз.
4. Management And Monitoring Tools терезесінде Network Monitor Tools (Средства сетевого монитора) (Желілік монитор қңралы) жалаушасын белгілейміз және ОК-ді шертіңіз.
5. Windows компоненттер шебері терезесінде Next-ті шертіңіз. Қажет болса Windows дискіні енгізіңіз немесе қажетті файлдарға жолды көрсетіңіз.
6. Орнатуды аяқтау ншін Finish (Готово) (Дайын) батырмасын шертіңіз.

Желілік монитор драйверін орнатыңыз:

1. Start\Settings\Control Panel мәзірін ашыңыз және Network and Dial-Up Connections (Сеть и удаленный доступ к сети) (Желі және желіге кіру жойылған) жарлығын шертіңіз.
2. Жергілікті қосылуда мониторингін орындау үшін оң жақ батырманы шертіңіз және контекстік мәзірде Properties (Свойства) (Қасиет) бұйрығын таңдаңыз.
3. Жергілікті қосылудың қасиеттері терезесінде Install (Установить) (Орнату) батырмасын шертіңіз.

4. Select Network Component Type (Выбор типа сетевого компонента) (Желілік компонент типін таңдау) терезесінде Protocol-ды (Протокол) (Хаттама), ал одан кейін Add (Добавить) (Толықтыру) батырмасын шертіңіз.
5. Select Network Protocol (Выбор сетевого протокола) (Желілік хаттаманы таңдау) терезесінде Network Monitor Driver (Драйвер сетевого монитора) (Желілік монитор драйверін) таңдаңыз және ОК-ді шертіңіз. Қажет болса Windows дискіні енгізіңіз немесе қажетті файлдарға жолды көрсетіңіз.

TCP тізбектілігін қарап шығыңыз:

1. Network Monitor-ды жіберіңіз.
2. Жазылған деректерді қарап шығыңыз.
3. Display (Отображение) (Бейнелеу) мәзірінде Options (Параметры) (Параметрлері) бұйрығын таңдаңыз.
4. Auto-ны (based on protocols in the display filter) [Авто (на базе протоколов фильтра отображения) (Хаттамалар базасындағы бейнелеу сүзгісі)] таңдаңыз және ОК-ді шертіңіз.
5. Display мәзірінде Filter (Фильтр) (Сүзгі) бұйрығын таңдаңыз.
6. Protocol=Any жолын екі рет шертіңіз.
7. Protocol салымшасында Disable All (Отключить все) (Барлығын алып тастау) батырмасын шертіңіз.
8. Disabled Protocols (Отключенные протоколы) (Ажыратылған хаттамалар) тізімінде TCP таңдаңыз.
9. Enable (Включить) (Қосу) батырмасын, ал одан кейін ОК-ді шертіңіз.
10. Capture (Запись) (Жазу) мәзірінде Start (Запустить) (Жнргізу) бұйрығын таңдаңыз.

Қосылуды жасау:

1. Start\Programs\Administrative Tools мәзірін ашыңыз және Terminal Services Configuration (Настройка служб терминалов) (Терминалдар қызметін баптау) жарлығын шертіңіз.
2. Connections (Подключения) (Қосу) бумасын оң жақ батырмасымен шертіңіз және контекстік мәзірде Create New Connection (Создать подключение) (Қосылуды жасау) бұйрығын таңдаңыз. Terminal Services Connection (Мастер подключения к службам терминалов) (Терминалдар қызметтеріне шебердің қосылуы) шебер терезесі ашылады.
3. Next-ті шертіңіз.
4. Шебердің бірінші терезесінде қосылу түрін таңдаңыз, мысалы Microsoft RDP 5.0 және Next-ті шертіңіз.
5. Шифрлау деңгейін таңдаңыз: Low, Medium немесе High (Низкий, Средний немесе Высокий) (Төменгі, Орта немесе Жоғарғы). Windows тың нақтылысын әдеттегідей тексеруге болады. Next-ті шертіңіз.
6. Параметрлерді және алыстан басқару деңгейін беріңіз және Next шертіңіз.

7. Қосылудың атын, хаттама түрін, коментарийді көрсетіңіз және Next-ті шертіңіз.
8. Берілген хаттама үшін бір немесе бірнеше желілік адаптерлерді таңдаңыз, рұқсатты қосылу санын беріңіз және Next-ті шертіңіз.
9. Finish батырмасын шертіңіз.

Терминалдар серверіне қатынауға рұқсат беру:

1. Start\Programs\Administrative Tools мәзірін ашыңыз және Computer Management (Управление компьютером) (Компьютермен басқару) жарлықты шертіңіз.
2. System Tools\Local Users And Groups\Users (Служебные программы Локальные пользователи и группы\Пользователи) (Қызметтік бағдарламалар Локалды қолданушылар мен топтар\Пайдаланушылар) түйінін ашыңыз.
3. Қатынауға рұқсат беруге қажет пайдаланушының объектісін екі рет шертіңіз.
4. Terminal Services Profile салымшысында Allow Logon To Terminal Server жалаушаны белгілеңіз және шертіңіз.
5. Computer Management жабдығын жабыңыз.
6. Start\Programs\Administrative Tools мәзірін ашыңыз және Terminal Services Configuration жарлығын шертіңіз.
7. Connections (Подключения) (Қосу) бумасында Rdp-Tcp-ті таңдаңыз.
8. Action (Действие) (Әрекет) мәзірінде Properties (Свойства) (Қасиет) бұйрығын таңдаңыз.
9. Permissions (Разрешения) (Рұқсат ету) салымшысын таңдаңыз және берілген терминалдар серверіне қатынауға рұқсаты бар пайдаланушыны немесе топты қосыңыз.
10. ОК-ді шертіңіз.
11. Terminal Services Configuration терезесін жабыңыз.

SNMP қызметін орнату:

1. Start\Settings\Control Panel мәзірін ашыңыз, Add/Remove Programs жарлығын шертіңіз және ашылған терезеде Add/Remove Windows Components батырмасын шертіңіз. Windows компоненттер шебері терезесі ашылады.
2. Management And Monitoring Tools-ты (Средства наблюдения и управления) (Бақылау және басқару құралы) компоненттер тізімінен таңдаңыз және Details (Состав) (Құрам) батырмасын шертіңіз. Management And Monitoring Tools диалогтың терезесі ашылады.
3. Simple Network Management Protocol жалаушасын белгілеңіз және ОК батырмасын шертіңіз.
4. Windows компоненттер шебері терезесінде Next батырмасын шертіңіз. Шебер SNMP хаттамасын орнатады.
5. Finish батырмасын шертіңіз.

Тапсырма 2:

1. IPSec хаттамасын зерделеу.
2. IPSec саясаты қасиеттерінің әр түрлі терезелерін сипаттау.
3. Аутентификация әдістерін сипаттау.
4. IP-пакеттерін сңзгілеуді сипаттау.
5. IPSec хаттамасы сүзгілерінің қызметін сипаттау.

Тапсырмасы бойынша компьютерде орындау:

Басқа компьютерлермен байланысын тексеру:

1. Басқа компьютердің IP-мекен-жайын көрсете отырып, Ping утилитасын іске қосыңыз.
2. Егер сіз төрт жауап алсаңыз, онда сіз өз әріптесіңізбен байланыса аласыз деген сөз.

MMC консоліне IPSec қосуды орындаңыз:

1. Start\Programs\Administrative Tools мәзірін ашыңыз және Local Security Policy (Локальная политика безопасности) (Локалды қауіпсіздік саясаты) жарлығын шертіңіз.
2. Консол ағашынан IP Security Policies On Local Machine (Политики безопасности IP на "Локальный компьютер") («Локалды компьютердегі» IP қауіпсіздік саясаты) таңдаңыз;
3. Оң жақ панельден Secure Server (Require Security) белгісін оң жақ батырмамен шертіңіз және контексті мәзірден Properties бұйрығын таңданыз.
4. Қасиеттер терезесінде Add (Добавить) (Толықтырып қосу) батырмасын шертіңіз. Қауіпсіздік ережелері терезесі ашылады.
5. Next батырмасын шертіңіз.
6. Tunnel Endpoint (Конечная точка туннеля) (Туннельдің ақырғы нүктесі) терезесінде Next шертіңіз.
7. Network Type (Тип сети) (Желілер типі) терезесінде Next шертіңіз.
8. Authentication Method (Метод проверки подлинности) (Түпнұсқалығын тексеру әдісі) терезесінде Use This String To Protect The Key Exchange (Preshared Key) (Использовать данную строку для защиты обмена ключами) (Кілттердің алмасуын қорғау үшін аталған жолды пайдалану) айырып-қосқышын шертіңіз. Төмендегі өріске MSPRESS теріңіз және Next батырмасын шертіңіз.
9. All IP Traffic (Весь IP-трафик) айырып-қосқышын шертіңіз, сосын Next батырмасын шертіңіз.
10. Require Security (Требовать безопасность) (Қауіпсіздікті талап ету) айырып-қосқышын шертіңіз, сосын Next батырмасын шертіңіз.
11. Шебер терезесін жабу үшін Finish (Готово) (Дайын) батырмасын шертіңіз.
12. Енді сүзгінің қатаң тізімін қосқаннан кейін үнсіздік бойынша барлық сүзгілерді істен шығарыңыз.
13. Secure Server (Require Security) Properties диалог терезесін жабыңыз.

14. Secure Server (Require Security) оң батырмасымен шертіңіз және контексті мәзірден Assign (Назначить) (Тағайындау) бұйрығын таңданыз.
15. Екінші компьютер мекен-жайын көрсете отырып Ping утилитасын іске қосыңыз.
16. Желі бойынша байланыс мүмкін болуы үшін, контекст мәзір көмегімен Secure Server (Require Security) саясатын істен шығарыңыз.

Тапсырма 3:

1. IPSec ережелері мен саясатын сипаттау.
2. Брандмауэрлермен, NAT-пен және прокси-сервермен жұмыс жасау үшін IPSec-ті баптау үдрісін сипаттау.
3. Басқару утилиттерін зерделеу.
4. Network Monitor көмегімен шифрланбаған трафикті қарау.

Тапсырмасы бойынша компьютерде орындау:

IPSec өзіндік саясатын құрыңыз:

1. Start\Programs\Administrative Tools мәзірін ашыңыз және Local Security Policy жарлығын шертіңіз.
2. Терезенің сол жағында IP Security Policy On Local Machine белгісін оң батырмамен шертіңіз.
3. Create IP Security Policy бұйрығын контекстік мәзірде таңдаңыз.
4. Шеберді іске қосқаннан кейін жалғастыру ншін Next батырмасын шертіңіз.
5. Саясат атын енгізіңіз. Two Computer Policy және Next батырмасын шертіңіз.
6. Requests For Secure Connection терезесінде Default Response Rule жалаушасын босатпай Next батырмасын шертіңіз.
7. Kerberos хаттамасы арқылы аутентификациялау үшін нақтылығын тексеру тәсілін үнсіз келісіммен өз қалпында қалдырыңыз.
8. Edit Properties жалаушасы ерекшеленіп тұрғанына көз жеткізіңіз.
9. Бастапқы баптауды аяқтау үшін Finish батырмасын шертіңіз.
10. Қасиет терезесі ашылады: ОНЫ ЖАППАҢЫЗ! Бұл атқарылған жұмыстың әлі ережесі құрылған жоқ, тек жауаптың қасиеттері анықталды. Әрі қарай IP Sec саясаты шеберсіз қолмен дайындалады.

Жаңа ережені қосыңыз:

1. Қасиет диалог терезесінің астыңғы жолағында Use Add Wizard (шеберді шақыру) жалаушасын түсіріңіз.
2. Rules салымшасында Add батырмасын шертіңіз.
3. Жаңа ережелер қасиетінің терезесі ашылады.
   Сіз компьютерлер арасында мәлімет алмасу снзгілерін баптадыңыз. Қазір өз компьютерлеріңіздің IP – мекен-жайын, бастапқы мекен-жайын және екінші компьютер IP – мекен-жайын соңғы мекен-жай ретінде көрсетіп шығу сүзгісін жасадыңыз.

Жаңа сүзгіні қосыңыз:

1. Add батырмасын шертіңіз, IP Filter List диалог терезесі ашылады.
2. Name өрісінде сүзгі атын еңгізіңіз – Host A-Host B Filter.
3. Use Add Wizard жалаушасын өшіріңіз.
4. Add батырмасын шертіңіз, сүзгі қасиеті терезесі ашылады.
5. Source Address өрісінде нақты IP – мекен-жайын енгізіңіз.
6. Өзіңіздің IP мекен-жайыңызды қосыңыз.
7. Destination Address өрісінде нақты IP – мекен-жайын енгізіңіз.
8. Екінші компьютердің IP – мекен-жайын енгізіңіз.
9. ОК батырмасын шертіп,тексеріңіз.
10. Close батырмасын шертіңіз.
11. IP Filter List салымшысында жаңа сүзгінің белсенділігін арттырыңыз.
    Алдыңғы тапсырмада сіз кіріп-шығу сүзгілерін жасадыңыз, ал енді бумаларды сүзгілеу іс әреккеті анықталады.

Снзгілерді іске қосыңыз:

1. Filter Action салымшасына көшіңіз де, Use Add Wizard жалаушасын түсіріңіз.
2. Add батырмасын шертіңіз.
3. Security Methods салымшасында Negotiate Security жалаушасының белгіленгеніне көз жеткізіңіз.
4. Allow Unsecured Communication With Non IPSEC Aware Computer жалаушасының түсірілгендігіне көз жеткізіңіз.
5. Қорғау әдісін таңдау үшін Add батырмасын шертіңіз.
6. Medium (AH) таңдап, ОК батырмасын шертіңіз.
7. ОК батырмасын шертіңіз, содан соң диалог терезесі жабылады.
8. Сүзгілерді іске қосатын айырып-қосқышты шертіңіз.
   Содан соң екі компьютер арасында сенімді қарым-қатынас орнатылады. Сіздердің қорғанысыңыз код сөзі немесе код сөз тіркесі болады.

Аутентификация әдісін таңдаңыз:

1. Authentication Methods салымшысына көшіңіз.
2. Add батырмасын шертіңіз.
3. Pre-Shared Key алмастыру батырмасына бір рет шертіңіз.
4. Мәтіндік өрісте дайын кілтті немесе парольді енгізіп, ОК-ді шертіңіз.
5. Pre-Shared Key тізімінде Move Up батырмасын шертіңіз, осы элемент бірінші болуы үшін.

Туннель параметрлерін тексеріңіз:

1. Tunnel Setting салымшысына көшу керек.
2. This Rule Does Not Specify An IPSEC Tunnel айырып-қосқышы таңдалғанына көз жеткізіңіз.

Қосылу типінің параметрлерін тексеріңіз:

1. Connection Type салымшысына көшіңіз.

2. All Network Connections айырып-қосқышы таңдалғанына көз жеткізіңіз.

Ережені құруды аяқтаңыз:

1. Саясат параметрлерінің терезесіне қайтып бару үшін Close батырмасын шертіңіз.
2. Сіздің жаңа ережеңіз тізімде белгіленгеніне көз жеткізіңіз.
3. Саясат қасиеттері терезесін жабыңыз.

Жаңа саясаттың белсенділігін арттырыңыз:

1. Two Computer Policy батырмасын шертіңіз.
2. Assign батырмасын шертіңіз.
3. Policy Assigned бағанында енді Yes пайда болады.

IPSec-ті тестілеңіз:

1. Екі компьютерде де саясатты қосыңыз.
2. Екінші компьютер мекен-жайын көрсетіп, Ping утилитін іске қосыңыз.
3. Ең бірінші жіберілген сұраныс әзірше өтпейді.
4. Екі компьютерге де сай саясат қосылғаннан кейін,тестілеу тез, әрі оңай өтеді.
5. Бір компьютерде саясатты қосып және өшіріп, не боларын көруіңізге болады.

IPSec толықтық пакеттерін қарап шығыңыз (AH формат негізінде):

1. Network Monitor іске қосыңыз да, компьютерді екінші жүйемен байланыстыратын жүйелік төлемнің MAC-мекен-жайына тор орнатып қойыңыз. Айта кету керек: желілік адаптердің MAC-мекен-жайын көру үшін all параметрлі ipconfig утилитін іске қосыңыз.
2. Local Security Settings қойылымында Two Computer Policy саясатын белгілеңіз.
3. Network Monitor арқылы пакеттің алдын алуды бастаңыз.
4. Ipsecmon уттилитін іске қосыңыз.
5. IP мекен-жайын анықтай отырып, ping утилитін іске асырыңыз. Сізге осы әрекет қатарын қайталау керек болады.
6. Network Monitor-ды тоқтатып, тізімді қарап шығыңыз.
7. Ipsecmon-ды қарап шығыңыз.
8. ICMP бірінші пакетті екі рет шертіңіз.
9. Ethernet, IP және AH тақырыптары көрсетілген жолдарға көңіл аударыңыз.
10. IP жазылымын анық жазылған облысында жазып ашыңыз.
11. IP хаттамасының нөмірін көрсетіңіз. Ipsec IP, ICMP және Data жолдарының негізінде ICV құрылды. Бұл хабарламалардың алынып қалуына, өзгертілуіне, қайта алмасуына жол ашады. Hex панелін қарап шығып, сіз тағы 32 белгі көресіз, оларды ping жіберді. AH қорғанысын пайдалана отырып, сіз қауіпсіздікті қамтамасыздандырасыз, бірақ хабарламаның шифрлануын қамтамасыз етпейсіз.

ESP шифрлауын жөндеңіз:

1. Two Computer Policy саясатын белгілеңіз.
2. Two Computer Policy саясатының өзгеріс терезесінде Properties бұйрығын контексті мәзірден таңдап орындаңыз.
3. Filter Action қойылымына көшіңіз.
4. Сүзгінің белсенділігін өзгертіңіз.
5. Edit батырмасын өзгерістер енгізу үшін шертіңіз.
6. High (ESP) таңдаңыз.
7. Диалог терезелердің барлығын жабыңыз.
8. Two Computer Policy саясатын белгілеңіз.

Шифрланған IPSec пакеттерін қарап шығыңыз:

1. Network Monitor арқылы алып қалуды іске асыруды бастаңыз.
2. Ipsecmon утилитін іске қосыңыз.
3. Екінші компьютердің IP мекен-жайын көрсетіп, ping утилитін іске қосыңыз.
4. Осы әрекет қатарын қайталауңызға тура келеді. Мәселен, екі компьютер арасында қауіпсіздік қатарын келтіру үшін уақыт керек.
5. Network Monitor тізімін тоқтатып, көріп шығыңыз.
6. Ipsecmon-ды қарап шығыңыз.
7. ESP кадрын екі рет шертіңіз.
8. IP хаттамасын жазыңыз.
9. IP анықтамасының терезесін жылжыта отырып, IP Data: Number Of Data Bytes Remaining – 76 (Ox004C) шертіңіз. Hex панелінде шифрланған мәлімет қатарын көресіз.

IPSec белсенділігін қарап шығыңыз, SA белсенділерін қарап шығыңыз:

1. Control PaneI терезесінде Network and Dial-Up Connections белгілеңіз.
2. Local Area Connection белгілеп, контексті мәзірдегі Properties бұйрығын таңдаңыз.
3. Internet Protocol (TCP/IP) таңдаңыз, Properties батырмасын шертіңіз.
4. Advanced батырмасын шертіңіз.
5. Options(параметрлер) қойылымынан өтіп, IP Security және Properties батырмасын шертіңіз.

Компьютер локалды саясат ұстанса Usi1: This IP Security Policy атындай жол пайда болады. Егер Active Directory тобы механизмінің саясатын қолданса, онда жолдарды қолдана алмайды, бірақ саясат аты сол жолда жазылып шығады.

Бақылау сұрақтары

1. OSI эталондық моделі дегеніміз не?
2. Деңгейдің мақсаттары мен қызметтері.
3. Желілік хаттамалардың қызметі.
4. Екі деңгей арасындағы интерфейс дегенді қалай түсінесіз?
5. Десте дегеніміз не?

6. Десте қандай бөліктерден тұрады?
7. Ең жоғары деңгей және оның қызметі.
8. Ең төменгі деңгей және оның қызметі.
9. Деректердің форматтарын ауыстыру қай деңгейге жүктелген?
10. Деректерді жеткізуде қысқа жолды ұйымдастыру қай деңгейге жүктелген?
11. Ашық жүйеге анықтама беріңіз.
12. Қолданбалы бағдарлама OSI моделінің қай деңгейінде жұмыс істейді?
13. Желілік қызметтер OSI моделінің қай деңгейінде жұмыс істейді?
14. Қай ұйым Ethernet желілерінің стандарттарын құрастырды?
15. Транспорттық және ақпараттық қызмет көрсетулерге анықтама беріңіз.
16. TCP/IP хаттамасының стегі дегеніміз не?
17. TCP/IP хаттамасының артықшылығы неде?
18. TCP/IP хаттамалар пакетінің архитектурасын сипаттаңыздар.
19. TCP хаттамасы жайлы айтыңыз?
20. IP хаттамасы жайлы сіз не білесіз?
21. UDP хаттамасы жайлы жалпы мәлімет.
22. SLIP хаттамасын сипаттаңыз.
23. PPP хаттамасын сипаттаңыз.
24. ARP хаттамасын сипаттаңыз.
25. IP хаттамасын сипаттаңыз.
26. ICMP хаттамасын сипаттаңыз.
27. UDP хаттамасын сипаттаңыз.
28. TCP хаттамасын сипаттаңыз.

Әдебиеттер тізімі

1. Дубовиченко С.Б. Компьютерные сети и Интернет. - Алматы: Данекер, 2001
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии; протоколы. – СПб.: Питер, 2006. – 692с.
3. Столингс В. Современные компьютерные сети. – СПб.: Питер,2004.
4. Гук М. Аппаратные средства локальных сетей. – СПб.: Питер, 2006.
5. Олифер В.Г. Компьютерные сети: учебное пособие. – Спб: Питер, 2008
6. Гусева А.И. Сети и межсетевые коммуникации. – М.: Диалог МИФИ, 2002
7. Таненбаум Э. Компьютерные сети. – Спб: Питер, 2007.
8. Спортак М. Компьютерные сети и сетевые технологии. – Спб: ООО ДиаСофт ЮП, 2005.
9. Компьютерные системы и сети: учебное пособие/ред.Косарев В.П. – М.: Финансы и статистика, 2000.