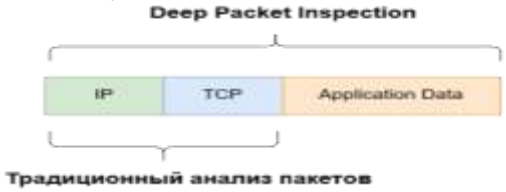
№ 4 Практикалық жұмыс. DPI – Deep Packet Inspection (Пакеттерді терең талдау)
Мақсаты: DPI технологиясын зерттеу.
Жоспары:
1. Теориялық бөлім: DPI технологиясын қолдана отырып бұғаттау.
2. Практикалық тапсырма

1. Теориялық бөлім: DPI технологиясын қолдана отырып бұғаттау.

DeepPacketInspection (қысқартылған: **DPI (пакеттерді терең талдау), сондай-ақ complete packet inspection** және **Information eXtraction немесе IX**) – бұл статистикалық мәліметтерді жинақтау, олардың мазмұны бойынша желілік пакеттерді тексеру және сүзу технологиясы. Брандмауэрлерден айырмашылығы, Deep Packet Inspection пакеттің тақырыптарын ғана емес, сонымен қатар екінші және одан жоғары OSI модель деңгейіндегі трафиктің толық мазмұнын талдайды. Deep Packet Inspection вирустарды анықтауға және бұғаттауға, сондай-ақ көрсетілген өлшемдерге сәйкес емес ақпаратты сүзуге қабілетті.
Deep Packet Inspection (DPI) - бұл желілік трафикті бақылау мен басқарудың озық әдісі. DPI - бұл пакеттерді нақты деректермен немесе жүктемелермен анықтайтын, сәйкестендіретін, жіктейтін, қайта бағыттайтын немесе бұғаттайтын пакеттерді сүзу (фильтрлеу) формасы. Оның дәстүрлі пакеттік сүзу формасынан айырмашылығы да осында. Өйткені, дәстүрлі пакеттік сүзу формасы (пакеттің тақырыптарын ғана тексереді) жоғарыда көрсеткендерді анықтай алмайды.
Әдетте, пакеттерді терең тексеру функциялары **OSI** моделінің қосымшалар деңгейінде (Application) жұмыс істейді, ал дәстүрлі пакеттік сүзу тек әр пакеттің тақырыбы туралы ақпарат береді. Қарапайым тілмен айтсақ, дәстүрлі пакеттік сүзу кітаптың атауын ғана оқу, яғни ішіндегі мазмұнын түсінбей немесе бағаламай оқу сияқты.



DPI ҚАЛАЙ ЖҰМЫС ІСТЕЙДІ?
DPI көрсетілген нүктеден өтетін пакеттердің мазмұнын тексереді және пакеттің құрамына байланысты компания, провайдер немесе желі әкімшісі тағайындаған ережелер негізінде нақты уақыт режимінде шешім қабылдайды. Соңғы уақытқа дейін фаерволдар нақты уақыт режимінде трафиктің ауқымды көлемін тереңірек талдау үшін қажетті есептеу қуатына ие болмады.
Пакеттерді терең талдау келген хабарламалардың мазмұнын тексеріп, хабарламалар келген нақты қосымшаны немесе қызметті анықтай алады. Сонымен қатар, сүзгілерді желілік трафикті белгілі бір Интернет-

хаттамасының (IP) адрестерінен немесе Facebook сияқты белгілі бір онлайн қызметтен іздеу және қайта бағыттау үшін программалауға болады.

DPI ҚАЛАЙ ҚОЛДАНЫЛАДЫ?

Пакеттерді терең тексеруді желілік трафик ағынын оңтайландыру үшін желіні басқару кезінде қолдануға болады. Мысалы, жоғары басымдықты деп белгіленген хабарлама аса маңызды емес немесе басымдығы төмен хабарламаларға немесе Интернетті қарау кезінде кездейсоқ кездесетін пакеттермен салыстырғанда межелі жерге ертерек жіберілуі мүмкін. DPI-ді p2p-дің теріс пайдаланылуын болдырмау үшін трафикті азайту үшін пайдалануға болады, бұл желінің жұмысын жақсартады.

Сондай-ақ, DPI корпоративті желіге червьтердің (құрттардың), шпиондық бағдарламалар мен вирустардың енуіне жол бермеу үшін қолданылады. Осымен бірге, DPI-ді құрылғылардан зиянды сұраныстарды бұғаттау арқылы DDoS шабуылдары кезінде IoT құрылғыларын пайдалануды болдырмау үшін интернет-провайдерлердің мүмкіндіктерін кеңейту үшін де қолдануға болады. Пакеттерді терең талдау буфердің толып кету шабуылдарының кейбір түрлерінің алдын алады.

Сондай-ақ, пакеттерді терең талдау ақпараттың жария болуына (утечка) жол бермейді, мысалы, құпия файлды электрондық пошта арқылы жіберген кезде. Файлды сәтті жіберудің орнына, пайдаланушы қажетті рұқсатты және оны жіберуге рұқсатты қалай алуға болатындығы туралы ақпарат алады.

DPI ТЕХНИКАСЫ

Пакеттерді терең талдауда қолданатын негізгі екі өнім түрі бар: кіруді анықтау жүйесі (IDS), мысалы, мазмұнды тексеру, және тек шабуылдарды анықтамай, желіңізді қорғауға бағытталған IDS мүмкіндіктерін іске асырады. Пакеттерді терең тексеру үшін қолданылатын кейбір негізгі әдістерге мыналар жатады: Өнімнің екі негізгі түрі пакеттерді терең тексеруді қолданады: мазмұнды тексеру сияқты IDS (Intrusion Detection System – кіруді анықтау жүйесі) және шабуылдарды анықтаумен қатар, желіні қорғауға бағытталған IDS жүйелері сияқты функцияларды жүзеге асыратын желіаралық экрандар. Пакеттерді терең талдау үшін қолданылатын кейбір негізгі әдістерге мыналар жатады:

- Үлгі немесе сигнатур (Pattern or signature matching) сәйкестігі – IDS функцияларын қолданатын фаерволдарды қолданудың бір тәсілі белгілі желілік шабуылдардың мәліметтер базасына негізделген әр пакетті талдайды.
- Бұл тәсілдің кемшілігі мынада: ол әлі анықталмаған шабуылдар үшін емес, белгілі шабуылдар үшін ғана тиімді.
- Хаттама аномалиясы (Protocol anomaly) - IDS функциялары бар фаэрволдарды қолданудың өзге тәсілі, хаттама аномалиясы қауіпсіздіктің негізгі қағидасы болып табылатын "әдепкі тыйым салу" тәсілін қолданады. Бұл техникада хаттама анықтамалары (protocol definitions) қай контентке рұқсат етілетінін анықтау үшін қолданылады. Бұл тәсілдің басты артықшылығы – ол белгісіз шабуылдардан қорғауды қамтамасыз етеді.

- IPS шешімдері – кейбір IPS шешімдері (Intrusion Prevention System-басып кіруді болдырмау жүйесі) DPI технологиясын қолданады. Бұл шешімдер IDS-ге ұқсас мүмкіндіктерге ие, бірақ олар нақты уақыт режимінде анықталған шабуылдарды бұғаттай алады. Бұл әдісті қолданудағы ең үлкен проблемалардың бірі – консервативті саясат құру арқылы белгілі бір дәрежеде азайтуға болатын жалған позитивтер қаупі.

Осы және басқа DPI әдістеріне кейбір шектеулер бар, дегенмен жеткізушілер практикалық және архитектуралық мәселелерді әртүрлі жолдармен шешуге бағытталған шешімдерді ұсынады. Сонымен қатар, DPI шешімдері қазір VPN, зиянды бағдарламаларды талдау, спамға қарсы сүзу, URL адрестерін сүзу және желіні қорғаудың басқа технологиялары сияқты бірқатар қосымша технологияларды ұсынады.

DPI КЕМШІЛІКТЕРІ

Мінсіз технология жоқ, технологиялардың бәрінен кемшілік табуға болады. DPI-дің де өзге технологиялар секілді кемшіліктері бар. Оның бірнеше әлсіз тұсын атап өтейік:

- Пакеттерді терең тексеру "техникалық қызмет көрсетуден бас тарту" шабуылдары, буферлік шабуылдар және тіпті зиянды бағдарламалардың кейбір түрлері сияқты шабуылдардың алдын алу үшін өте тиімді. Бірақ оны осындай шабуылдарды жасау үшін де қолдануға болады.
- Пакеттерді терең тексеру сіздің қазіргі фаерволыңызды және сіз қолданатын басқа қауіпсіздік программаларын басқаруды қиындатуы мүмкін. Сіз үнемі тиімділікті қамтамасыз ету үшін пакеттерді терең тексеру саясатын әрдайым жаңартып отыратындығыңызға сенімді болуыңыз керек.
- Пакеттерді терең тексеру фаерволға өңдеу жүктемесімен жұмыс істей алуы үшін ресурстарды бөліп беруіне байланысты желінің жұмысын баяулатуы мүмкін.

Құпиялылық мәселелері мен пакеттерді терең тексерудің ішкі шектеулерінен басқа, https сертификаттарын және тіпті vpn туннельдерін пайдалану кезінде бірқатар мәселе туындады. Қазір кейбір фаерволдар HTTPS-пен қорғалған трафикті шифрлайтын және контентті өткізіп жіберуге болатындығын анықтайтын HTTPS талдауын ұсынады. Алайда, пакеттерді терең талдау өнімділікті басқарудан бастап, желіні талдауға, сараптама мен кәсіпорынның қауіпсіздігіне дейінгі көптеген мақсаттар үшін құнды практика болып қала береді.

Deep Packet Inspection пакеттердің мазмұны бойынша ғана емес, сонымен қатар белгілі бір желілік программалар мен хаттамаларға тән жанама белгілер бойынша да шешім қабылдай алады. Ол үшін статистикалық талдауды қолдануға болады (мысалы, белгілі бір таңбалардың жиілігінің статистикалық талдауы, пакеттің ұзындығы және т.б.).

Deep Packet Inspection-ды провайдерлер көбінесе трафикті бақылау үшін, кейде BitTorrent сияқты кейбір хаттамаларды бұғаттау үшін пайдаланады. Deep Packet Inspection көмегімен деректерді қандай қосымшаның жасағанын немесе алғанын анықтап, соның негізінде қандай әрекет ету қажеттігін білуге болады. Бұғаттаудан басқа, Deep Packet Inspection ежей-тегжейлі статистиканы әр пайдаланушы үшін бөлек жинақтай алады. Сондай-ақ, quality of service Deep Packet Inspection көмегімен жеке пакеттердің берілу жылдамдығын оны көтеру немесе керісінше азайту арқылы басқара алады. Кейбір интернет-провайдерлердің пікірінше, Deep Packet Inspection Интернет-каналды бітеп тастайтын қосымшаларды тежеуге, әртүрлі деректерді беру басымдықтарын өзгертуге мүмкіндік береді, мысалы, ауқымды (үлкен) файлдарды жүктеу жылдамдығын азайту арқылы Интернет беттерін ашуды жеделдетуге болады.

Сонымен қатар, Deep Packet Inspection, өндірушілердің дәлелденбеген мәлімдемесіне сәйкес, трафиктің жалпы ағымының ішінен компьютерлік вирустарға сәйкес келетін бөліктерді анықтап, оларды бұғаттай алады, осылайша желінің қауіпсіздігін арттырады. Кейде Deep Packet Inspection ірі корпорацияларда деректердің кездейсоқ жария болып кетуіне жол бермеу үшін, сондай-ақ ішкі қорғалған файлдарды электрондық пошта арқылы жіберуден қорғау үшін қолданылады.

Программалық қамтамасыз ету

Hippie (Hi-Performance Protocol Identification Engine) –Deep Packet Inspection-ды C-те ашық бастапқы коды бар Linux үшін іске асыру.

L7-filter – бұл Deep Packet Inspection-ды OSI моделінің жетінші деңгейіндегі деректерді жіктеуге бағытталған C-тегі Linux үшін іске асырудың тағы бір тәсілі.

SPID (Statistical Protocol IDentification) — Deep Packet Inspection-ды C#-те ашық бастапқы коды бар Windows үшін іске асыру. OSI моделінің жетінші деңгейлі хаттамасын статистикалық трафикті талдау арқылы сәйкестендіреді.

2-ші практикалық тапсырма

1 Deep Packet Inspection технологиясын қолданатын кез-келген программалық қамтамасыз етуді қысқаша сипаттап беріңіз

2 Deep Packet Inspection технологиясын қолданатын құрылғы туралы қысқаша сипаттап беріңіз

3 Есеп түрінде жасаңыз.