Седемте слоя на мрежовата сигурност

Познаването на OSI модела е задължително за ИТ специалистите, за да могат да комуникират на един език с колегите си

Георги ЧОРБАДЖИЙСКИ, *вицепрезидент на Асоциацията за информационна сигурност ISECA*

Често се оказва, че проблемът в мрежовата сигурност е от типа PEBKAC (Problem Exists Between Keyboard and Chair) © „Ютилитис“

Нека започнем с няколко сценария, с които е възможно да се сблъскате:

1. *Получавате оферта от производител на мрежово оборудване, като в нея ви препоръчват да си закупите Layer 7 firewall.*

2. *Предлагат ви свързаност към голяма мрежа, но с уговорката, че свързаността е само Layer 2, а за Layer 3 трябва да се погрижите сами.*

3. *Имате проблем с мрежата си. Администраторът го решава, а на въпроса ви „какъв беше проблемът“ отговаря, че е имало проблем на Layer 8.*

Ако във всеки от горните сценарии ви става абсолютно ясно за какви слоеве (Layers) става въпрос, то вероятно от настоящата статия няма да научите нищо ново, тъй като в нея ще се разгледат основните мрежови слоеве. Запознавайки се с тези слоеве и какво се случва на всеки от тях, ще получите по-добро разбиране за вътрешната работа на съвременните компютърни мрежи.

Мрежовите устройства използват стотици официално дефинирани протоколи и технологии за комуникация. За да е объркването пълно, производителите изобретяват собствени протоколи и технологии и ги маркетират като по-по-най- в сравнение с общоприетите. Как в такава среда устройствата успяват да комуникират помежду си и да се разбират? А хората, ползващи технологиите, как се разбират, когато става дума за мрежи?

Решението е OSI (Open System Interconnection) моделът. OSI е модел, създаден от Световната организация за стандартизация (ISO) през 1984 г. OSI е концептуално разделение, което разбива процеса на изпращане на съобщение между два компютъра на седем поредни стъпки, наречени слоеве. Важно е да се отбележи, че моделът е концептуален, тоест в реалния свят слоевете не са реални или физически съществуващи. Те просто дефинират модела за представяне на мрежовите комуникации.

Въпреки че в повечето случаи няма нужда от пълно познаване на модела, частичното познаване е задължително за мрежовите администратори и IT мениджърите, за да могат ефективно да комуникират на един език с колегите си.

Веднъж запознали се с OSI слоевете, ще ви бъде по-лесно да решавате или да вниквате във възникналите мрежови проблеми, понеже всеки слой отговаря за една стъпка от процеса на изпращане на мрежово съобщение. Тези поредни слоеве работят независимо един от друг, без знанието какво става на другите слоеве. Единственото, което е нужно на даден слой, е знанието как да приема данни от по-горния и да ги предаде на по-долния слой.

OSI моделът дефинира седем слоя, по които се осъществява мрежовата комуникация.

слой 7 - Application (приложен)

Когато програма се нуждае от мрежова комуникация, първото нещо, с което се сблъсква, е приложният слой (Application layer). В контекста на OSI под приложен слой се няма предвид конкретна програма като Firefox - вашия уеббраузър, или Thunderbird - вашата пощенска програма, а протоколите, използвани от тези програми (в случая http, smtp, pop3 или imap). Представете си, че използвате програма за трансфер на файлове, за да изпратите файл на ваш колега. Тази програма комуникира с приложния слой и вероятно използва някой от протоколите на този слой (ftp, tftp, smb), за да изпрати файла ви. Накратко приложният слой позволява на програмите да взаимодействат с мрежата на най-високо ниво.

слой 6 - Presentation (представяне)

Този слой отговаря за представянето на данните в разпознаваем формат за приложния слой. На този слой се управляват компресията на данните, различните символни таблици, понякога и криптирането. Често този слой се прескача при създаването на мрежови приложения от ниско ниво, тъй като при тях не са необходими стъпки за конверсия на данните и обработка на данните от долните слоеве.

слой 5 - Session (сесиен)

Сесийният слой определя кога дадена сесия е била отворена, колко дълго е използвана и кога е затворена, като за идентификатори се ползват името на сесията и идентифицирането й по сигурен начин. С други думи, сесийният слой договаря и поддържа връзката на високо ниво с други устройства. Едни от най-често използваните протоколи на този слой са NetBIOS, употребяван за споделяне на файлове в Windows и RPC (remote procedure call) протокола.

слой 4 - Transport (транспортен)

На този слой се подготвят данните за изпращане през мрежата. Вашият компютър комуникира с получаващия данните компютър, като се решава как да се разделят данните в различни пакети, как да се подсигури предаването срещу загубата на пакети по пътя и как да се проверят пакетите от страна на получаващия. Транспортният слой осигурява среда за коректно предаване на данните и при нужда за разбиване на по-малки пакети и събирането им от страна на получателя. На този слой най-често ползваните протоколи са TCP (Transmission control protocol) и UDP (User datagram protocol).

слой 3 - Network (мрежови)

Мрежовият слой подсигурява преноса на данните между вашата мрежа и мрежата, с която комуникирате. Протоколите на този слой се грижат за маршрутизирането на пакетите от слой 4 и затова да бъде избран оптимален път за тяхното минаване между мрежите. На този слой най-често се ползват протоколите IP (Internet protocol) и IPv6, както и контролният протокол ICMP (Internet control message protocol).

слой 2 - Data Link (данни)

На този слой отдалеченият компютър бива обвързан с адрес в локалната мрежа. Слоят за данните се грижи за разпространението на данните единствено в локална мрежа. Целта на този слой е да капсулира данните във фреймове и да осигури безгрешно изпращане до един компютър, до който има локална връзка. На този слой са протоколите Ethernet, Token Ring, PPP и други.

слой 1 - Physical (физически)

На физическия слой се осъществява модулация на сигнала, носещ данните от горните слоеве. При изпращането на този слой данните могат да бъдат изпратени по различни видове кабели, безжично или дори чрез светлина (оптична връзка). В протоколите от този слой е знанието за волтажи, типове кабели, дължина на вълната и начините за модулация. Слой 1 се грижи физически данните да стигнат от един край до друг. На този слой са DSL, 100BaseTx, RS-232 и други.

Когато вашият компютър се нуждае от мрежова комуникация, той подава съобщение до приложния слой. Приложният слой избира протокол и предава данните към слоя за представяне, който от своя страна ги предава на сесийния слой и т.н. до физическия слой. Данните пътуват през OSI слоевете от седми към първи при изпращане и след получаването на данните от отсрещната страна - обратно нагоре отново до седми слой. За всеки от слоевете важи правилото, че знае само толкова, колкото му е нужно, за да си свърши работата, и нищо повече.

Въоръжени със знанията, изложени по-горе, можем да се върнем на сценариите в началото на статията и да разберем за какво става въпрос в тях.

В първия сценарий са ви оферирали firewall, който има възможност да филтрира и проксира протоколи на приложния слой. Един такъв firewall например има възможност да спира достъп до определени WWW сайтове (HTTP протокол) и да филтрира имейл съобщения (SMTP протокол).

При втория сценарий под Layer 2 свързаност се има предвид свързаност до мрежа за данни, като осигуряването на връзка през тази мрежа до доставчик на Layer 3 услуги (интернет) е ваша отговорност.

В третия пример се говори за проблем на Layer 8, но както видяхте, такъв слой всъщност не е официално дефиниран. Layer 8 е широко използвана шега в IT средите, като под layer 8 обикновено се има предвид човешкият фактор при ползването на мрежата. Проблемите на този слой най-често се описват с акронима PEBKAC, означаващ Problem Exists Between Keyboard and Chair, или с други думи - имате проблем, породен от човешка грешка или незнание.

OSI моделът предоставя удобен начин за описване на комплексни мрежови концепции бързо и без възможност за неразбирателство около базовата терминология. Дори и минималното познаване на модела помага в разнообразни ситуации, а по-дълбокото навлизане в подробностите ви позволява да избягвате ситуациите с проблеми на осми слой. ■