9. fejezet - Tartalom

9 *Sniffer*

A *snifferek* jelentik az egyik legnagyobb veszélyt a hálózatokra. Ebből a fejezetből kiderül, hogy mit is rejt ez a fogalom, melyek a snifferek felhasználási területei, és milyen gondokat okozhatnak.

9.1 Mi az a sniffer?

A *snifferekneknek* különböző felhasználási területeik vannak. Egyrészt a rendszergazdák pótolhatatlan segítőtársai a hálózati problémák vagy a potenciálisan veszélyeztetett területek felderítésében. Ha például gondok támadnak a hálózat egy részében a hiányos konfiguráció miatt, akkor a rendszergazda bevethet egy sniffert, hogy magállapítsa, hol van a probléma a hálózaton belül. Másrészt a snifferek lehetőséget nyújtanak a támadóknak, hogy egész hálózati csomagokat „hallgassanak le".

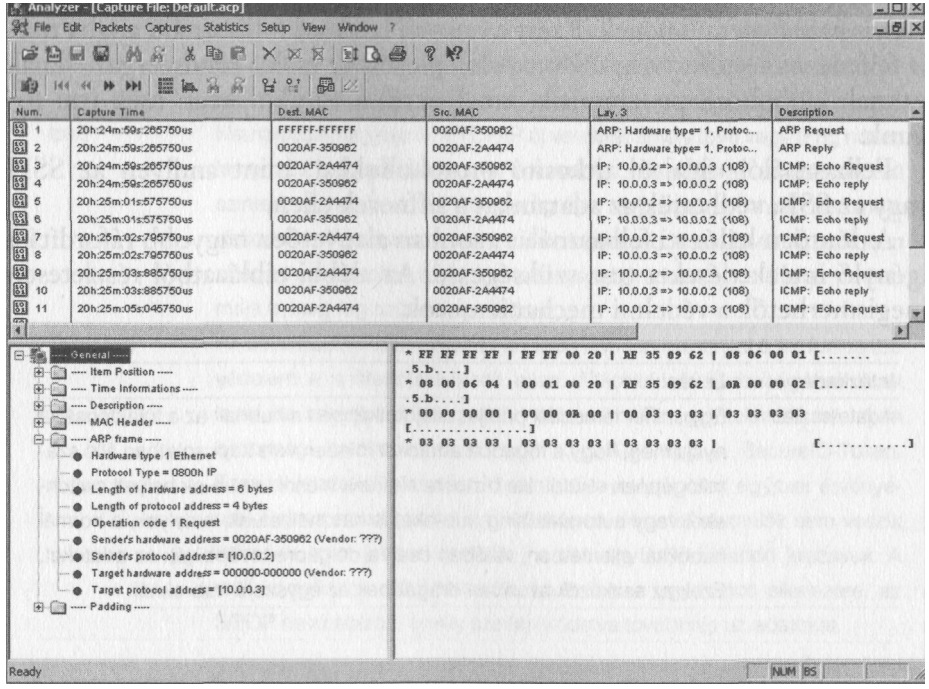
A snifferek a WWW/LAN/WAN egyes gépeire telepíthetők, naplózzák az adatfolyamot, és rendszerint egy fájlba írják az analizált adatokat, betekintést kínálva annak, aki installálta a sniffert.

A felhasznált sniffertől függően különböző protokollokat lehet lehallgatni. Ezek közé tartoznak többek között: a TCP/IP (Ethernet/WWW), az IPX, az Apple Talk, a Banyán VINES és az LCC.

9.2 Hogyan működik egy sniffer?

Egy számítógép valamennyi hálózati interfészének saját címe van a LAN-on. Ez különbözteti meg a komputert a hálózat többi tagjától. Hasonló rendszert találunk az internet-címzésnél is. A hálózatban gyakran használnak hub-ot az adatok szétosztására. Ha elküldünk egy üzenetet, az külön kis, *ethernet frame-nek* is nevezett csomagokban kerül a hub-ra, és onnan továbbítódik minden csatlakoztatott számítógépre. Az adatokat csak az a számítógép veszi fel, amelyiknek címezve vannak. A többi hálózati interfész ugyan fogadja az adatokat, de a nem neki szóló címzés miatt nem dolgozza fel azokat. Ezen a ponton avatkozik be a sniffer, amely a hálózati interfészt úgynevezett *promiscuous* módra állítja át. Ez a mód bizonyos alkalmazásokon keresztül akkor is megengedi a csomagok felvételét és feldolgozását, ha azok nem az illető gépnek vannak címezve. Így a sniffer hozzákezdhet a tulajdonképpeni munkájához.

Annak persze nem lenne értelme, hogy a hálózat teljes adatforgalmát kiértékelje, mert a legtöbb információ egyáltalán nem érdekes. Ezért a legtöbb sniffert úgy tervezték, hogy csak a *valóban releváns* adatokkal foglalkozzon. Ezek, a sniffer tulajdonságaitól függően, lehetnek például jelszavak vagy felhasználói nevek. Az elfogott információkat a sniffer az *output (kimeneti) fájlokba* menü.



Az Analyzer az egyik legismertebb sniffer

9.3 A sniffer veszélyei

A snifferek nagy veszélyt jelentenek a hálózati struktúrára, mert a teljes hálózati adatforgalmat felügyelhetik. Így azután nem is szükséges közvetlenül beavatkozni egy meghatározott felhasználó rendszerébe ahhoz, hogy kikémleljék mail-postafiókja vagy online banki jelszavát. Az olyan biztonsági intézkedések, mint hogy nem tároljuk a jelszavakat a merevlemezen, tulajdonképpen semmit sem érnek, mert ezeket bármikor megtudhatja a sniffer.

9.4 Mit lehet tenni a snifferek ellen?

A snifferek felfedezéséhez és eltávolításához jól kell ismerni a hálózati topológiát. A snifferek a normál felhasználó szempontjából semmilyen nyomot nem hagynak maguk után, ráadásul csak a támadó gépén futnak, vagyis *passzívan* működnek. Ezért a normál hálózati felhasználó aligha tudja felfedezni a sniffert a LAN-on. A leleplezéshez csak a rendszergazdáknak vannak különböző programjaik, amelyekről a továbbiakban még írni fogunk.

Felhasználói oldalról titkosító protokollokkal, mint amilyen az SSH vagy az SSL, védhetjük az adatainkat a siffherek ellen.

A döntően hálózati felhasználás azonban alapvetően nagyobb ráfordítást igénylő intézkedéseket tesz szükségessé. Az alábbi táblázatból részletesen megismerhetők a védelmi mechanizmusok.

Intézkedés	Leírás
Adatelosztás	Egy sniffer támadási pontját tulajdonképpen a hubnak az a tulajdonsága nyitja meg, hogy a fogadott adatokat minden vele kapcsolatban álló számítógépnek elküldi. Ha biztosra akarunk menni, a hub-ok helyett switcheket vagy auto-switching hub-okat is használhatunk, amelyek, a normál hubokkal ellentétben, valóban csak a célgépre továbbítják az adatokat. Ezek az eszközök azonban drágábbak az egyszerű hub-oknál.
Hálózati kártya	Egyszerűbb és olcsóbb megoldás megfelelő hálózati kártyával felszerelni a LAN-ra csatlakoztatott számítógépeket. Mivel egy sniffer csak úgy tud működni, ha a hálózati kártya promiscuous módban van, a megoldás kézenfekvőnek tűnik: csak olyan hálózati kártyát szabad használni, amely nem engedélyezi ezt a módot. Ilyen kártyákat (is) kínai pl. a 3Com, az IBM, a Hewlett-Packard és az Intel.
A csatlakozások ellenőrzése	A rendszergazda is ellenőrizheti a LAN-ban található számítógépek hálózati kártyáit promiscuous módra vagy egyéb gyanús alkalmazásokra. Ha azonban a támadó egy, a hálózatba integrált notebookot használ, amit a sniffelés után magával visz, ez a variáció, éppúgy, mint a fentiek, kevéssé hatékony.
A reakcióidő ellenőrzése	Ha egy számítógépre, amelynek a hálózati interfésze promiscuous módban van, adatokat küldenek, a reakcióideje hosszabb lesz az általában szokásosnál. Vannak programok, amelyek tesztelni tudják a hálózati reakcióidőket. Ezeket használják akkor is, amikor egy hálózat teljesítményének a gyenge pontjait keresik. Ha egy hálózatban rendszeresen tesztelik az egyes csatlakoztatott számítógépek reakcióidejét, akkor jól be lehet határolni azt a számítógépet, amelyik potenciális sniffer lehet.
Ipv6	Hamarosan megjelenik a TCP/IP új verziója, amely Ipv6 vagy IPng néven ismert. Ez a protokoll Ipsec-et is tartalmaz, amelynél az adatok hálózati szinten lesznek kódolva, mégpedig úgy, hogy csak a címzett gép tudja dekódolni. Részletesen most nem foglalkozunk az Ipv6-tal, azonban ahogy ez a protokoll majd szabvánnyá válik a hálón, a snifferek problémája is meg fog szűnni (egy időre).
Titkosítás	Az alkalmazásokban használt kódolás minden bizonnyal a legfontosabb védelem a sniffer-támadások ellen. Titkosítással biztonságossá lehet tenni az adatátvitelt. Nagyobb hálózatoknál megfontolandók az olyan biztonsági mechanizmusok, mint az S/Key vagy a SecureID-Token. Ezeknél jelszavak kiosztásáról van szó, amelyek csak egyszer érvényesek. Sajnos ez az eljárás elég költséges, és a felhasználók sem veszik szívesen, mert jobban szeretik, ha van egy saját, állandó jelszavuk. A mail-postafiókok elleni támadásoknak is van egy biztos ellenszere, az S/POP nevű eljárás, amely szintén kódolva továbbítja az adatokat.

Intézkedés	Leírás
SSL	A HTTP-átvitelek titkosítására szolgál az interneten az SSL (Secure Socket Layer). Már böngészőket is lehet kapni megfelelő erős kódolással. Az e-mail-küldésnél mindenesetre problematikus, hogy sok, csupán mail-szolgáltatást kínáló szolgáltató csak üzletileg kínálja az SSL használatát. Tehát figyelni kell arra, hogy milyen szolgáltatásokat veszünk igénybe a kevéssé biztonságos hálózatokon keresztül.
SSH	Mivel a Telnet kódolatlanul továbbítja az adatokat, például a jelszavakat és a parancsokat is, új lehetőséget kellett fejleszteni, hogy védetten lehessen bejelentkezni a Telnetről. A szokásos Telnet-kliensek helyett SSH-klienset (Secured Shell) is lehet használni, amely csak biztonságosan kódolva továbbítja az adatokat.
Anti-sniffer'	A hálón a legkülönbözőbb programokat kínálják a snifferek felkutatásához. Az olyan programok, amelyek azt a számítógépet ellenőrzik, amelyen éppen lokálisan rajta vagyunk, elérhetik ugyan a céljukat, de nincs nagy hasznuk. Vannak azonban olyan programok is, amelyek leleplezik, ha egy másik számítógép éppen sniffel. Ilyen program pl. Unixhoz/Linuxhoz a Beavis and Butthead, amely mint snifftest.c is ismert. Az ilyen programokkal szemben azonban mindig egy kicsit szkeptikusnak kell maradni, mert többnyire csak bizonyos hálózati kártyák búgjait ellenőrzik, vagy olyan programokat használnak, amelyek felhívják a figyelmet az ilyen támadásokra.

Védelmi Intézkedések a snifferek ellen

Végeredményben azonban mindig lesznek programok, amelyek ugyan hálózatról működnek, mégsem kínálnak lehetőséget az adatok kódolására. Mivel a legtöbb felhasználó nem szívesen használ manuális kódolást, a kódolási folyamatnak automatikusnak is kellene lennie.

A PGP-vel vagy hasonló programokkal kódolt fájlok/mailek biztonságában is csak akkor lehet bízni, ha a fájlok megnyitása a saját gépen történik. Ha azonban a PGP-vel kódolt maileket a mail-szerveren nyitják meg (ami biztosan gyakran megtörténik), akkor a megnyitáshoz szükséges jelszó megint csak a hálózaton megy keresztül, így ezt is minden sniffer foghatja. Igazán csak az IPv6 használatával lehet majd biztonságos adatátvitellel számolni, mivel ott az adatok eleve kódolva továbbítódnak, így a sniffer nem tud mit kezdeni velük.