SaveAs

Oktatási Anyag

Hálózati monitorozás, avagy
a csomag lehallgatás etikus és etikátlan felhasználása

Készült: 2001. február 11.

A dokumentum a fedőlappal együtt 21 számozott oldalt tartalmaz.

1. TARTALOMJEGYZÉK

OKTATÁSI ANYAG 1

1. TARTALOMJEGYZÉK 2

2. TEMATIKA 4

3. A CSOMAG LEHALLGATÁS ALAPJAI 6

3.1. Mi az a sniffelés? 6

3.2. Mi kell ahhoz, hogy sniffelni tudj? 6

3.3. A sniffelés elleni lehetőségek 7

4. MŰKÖDÉSI ELV 8

4.1. Mi az az Ethernet MAC address ? 8

4.2. Lehet-e változtatni a MAC address-emet? 8

4.3. Mi a csomaglehallgatás határai ? 8

5. MIB TÁMADÁS - SNIFFELÉS 9

5.1. Gyakorlati példák 1.a 9

5.2. Gyakorlati példák 1.b 10

5.3. Gyakorlati példák 2.a 10

5.4. Gyakorlati példák 2.b 11

5.5. Nem hálózati jellegű sniffelés, alkalmazás monitozorás 11

5.6. Alkalmazás monitozorás - példa 12

6. CSOMAG LEHALLGATÁS FELDERÍTÉSE 13

6.1. PING metódus 13

6.2. ARP metódus 13

6.3. DNS metódus 13

6.4. Source-route metódus 14
6.5. Decoy metódus 14
6.6. Host metódus 14
6.7. Lappangási metódus 15
6.8. TDR (Time-Domain Reflectometers) 15
6.9. Csomaglehallgatás felderítő szoftverek: 15
7. SNIFFELÉS SPECIÁLIS KÖRÜLMÉNYEK KÖZÖTT 16
7.1. Kábel modem/ DSL,ADSL szegmens sniffelése 16
7.2. Wireless, IEEE802.11 (AirPort) sniffelés 17
7.3. Sniffelés switchelt hálózaton. 18
8. HOGYAN LEGYÜNK „LEHALLGATÁS BIZTOSAK” 19
8.1. Idegen alkalmazás 19
8.2. Saját fejlesztésű alkalmazás 19
9. BIBLIOGRÁFIA 20
10. EGYÉB 21
10.1. Jelen dokumentum közlése 21
10.2. CopyRight 21

2. TEMATIKA

3. A csomag lehallgatás alapjai

- Mi az a „sniffelés”?
- Mi kell ahhoz, hogy sniffelni tudj?
- És hogy ne tudjanak sniffelni?

4. A csomag lehallgatás működési elve

- Milyen eszközök szükségesek hozzá?
- Mi az az Ethernet MAC address?
- Lehet-e változtatni a MAC addressemet?
- Mik a csomaglehallgatás határai?

5. Man in the middle attack

- Mi az a Man in the middle attack?
- Egyéb (hálózati) módszerek:
  - Adatmanipuláció, forgalom átvétel
- Egyéb (nem hálózati) módszerek:
  - Módosított kód elve
  - Alkalmazás „monitorozása”
  - A jelszó paramétereinek kinyerése titkosított adatfolyamból

6. A csomag lehallgatás felderítése

- Általános információk
- Ping metódus
- ARP metódus
- DNS metódus
- Source-routing metódus
- Decoy metódus
- Host metódus
- Lappangási metódus
- TDR
- HUB ledek
- SNMP monitoring
- Eszközök a sniffelés felderítésére

7. Sniffelés speciális körülmények között

- Kábelmodem (tv) sniffelési lehetőségei
- DSL, ADSL sniffelési lehetőségek
- Wireless, IEEE802.11 (AirPort) sniffelési lehetőségek
- Switchelt hálózat sniffelhetősége
- Receive-only eszköz készítése, a tökéletes megoldás?

8. Hogyan legyünk „lehallgatás biztosak”

- Idegen alkalmazás
  - Egyértelmű protokollok
  - Protokoll Analízis
- Saját fejlesztésű alkalmazás
  - Mire ügyeljünk?
  - Titkosítás, hitelesítés, jogosultsági szintek, mi kell még?

3. A CSOMAG LEHALLGATÁS ALAPJAI

3.1. Mi az a sniffelés?

Célja a hálózati forgalmak lehallgatása, hálózati forgalomban szenzitív információk keresése

A „hagyományos sniffelés” elvének alapjai: Az Ethernet, a MAC address és a hálózati kártyák promiscuous mode lehetősége

Általános céljai:

- cleartext jelszavak megszerzése,
- hálózati forgalom ember által olvasható formába konvertálása,
- hálózati hibák felderítése,
- hálózat terhelhetőség/terhelés analizálásának lehetősége,
- hálózati behatolások (hacker/cracker) felderítése,
- hálózati forgalom naplózása számlázáshoz analízisekhez (ISP)

3.2. Mi kell ahhoz, hogy sniffelni tudj?

Hardver:

- Egy hardware; mely a legtöbb esetben egy számítógép, de léteznek céleszközök is (Handheld + 2 pcmcia ETH dev, stb.)
- Hálózati eszköz; mely képes a hálózati forgalmat fogadni és feldolgozni, esetleg abba beavatkozni. Ez legtöbb esetben egy hálózati kártya, vagy az adott hálózat kommunikációját biztosító eszköz (kábelmodem, ADSL modem, wireless adapter, stb.)

Szoftver:

- A „packet capture” szoftver, mely képes tárolni az átmenő adatokat, képes azokat realtime értékelni, esetleg módosítani. Ez elég változatos lehet az adott feladattól függően.

3.3. A sniffelés elleni lehetőségek

Alkalmazott titkosítási / hitelesítési megoldások:

- SSL "Secure Sockets Layer" (plaintext adatcsatornák titkosítására stunnel, vagy kész megoldás használata, pl. az SSN-sFTP)
- PGP and S/MIME (GnuPG vagy PGP, X.509 használata esetén openssl és smime)
- Ssh „Secure Shell”
- VPNs (Virtual Private Networks)

A jelszavak védelmének lehetőségei:

- SMB/CIFS esetén: Sambav2 vagy NT >SP3 alkalmazása, a régi gyenge LanManager titkosítás elkerülése érdekében
- Kerberos V5: Mind a Win2k, mind a legtöbb unix támogatja a kerberos authentikációt, így vegyes környezetben is jól használható. (A win2k nem teljesen kompatíbilis, de a legtöbb unix már támogatja)
- Smartcard, tokens: bármilyen eszköz megfelelő amely automatikusan képes onetimepassword/chalange-response generálására. Esetleg szóba jöhetnek magasabb szintű authentikációk is. (PKI)

4. MŰKÖDÉSI ELV

4.1. Mi az az Ethernet MAC address ?

Az ethernet alapú hálózati eszközök rendelkeznek egy MAC address-szel, ez a címet a hardware gyártója határozza meg, mely ilyen formán egyedi azonosítója a csomagnak. A MAC cím szerepe a hálózati forgalom egyedi azonosítója, mely alacsony szinten meghatározza, hogy melyik csomagnak melyik géphez kell tartoznia.

A MAC address egy 12 számjegyből álló hexadecimális számsor, mely minden különálló ethernet kommunikációs eszköznél egyedi.

Miért van szükség a MAC-ra ha ott van az IP?

Az IP más szinten kapcsolódik a csomaghoz. Ez egy magasabb szint az OSI szabvány szerint. A hálózat irányító eszközök nem IP szinten vizsgálják a csomagokat, hiszen léteznek olyan protokollok, ahol az IP nem is létezik (pl. az IPX protokoll). Továbbá az eseten nagy többségében az IP cím nem egyedi, és a megváltoztatása is egyszerű, mely jelenthetne problémát egy hálózati forgalom irányító eszköznek mondjuk egy DHCP környezetben.

4.2. Lehet-e változtatni a MAC address-emet?

A válasz igen! Sőt, nagyon egyszerűen, a legtöbb hálózat lehallgatási megoldásnak az alapja a MAC módosítás, hamisítás.

Ugyan a MAC address-t a hálózati kártya helyezi el az ethernet frame-ben, de legtöbb hálózati egység alapból felkínálja a runtime MAC address újrakonfigurálást.

Ez nem hiba, sok-sok eszköznél (tűzfalak, forgalom irányítók) ez létszükséglet a működéshez.

4.3. Mi a csomaglehallgatás határai ?

A hagyományos értelemben vett csomag lehallgatás esetében, fontos, hogy a csomag lehallgató eszköz fizikailag szerepeljen abban a hálózatban, amelyen áthalad a lehallgatni kívánt csomag. Tehát nem kell, hogy a csomaglehallgatás a végponton vagy a kezdőponton történjen; elég ha a két pont közötti hálózatot összekötő hálózati rendszerhez van hozzáférés.

5. MIB TÁMADÁS - SNIFFELÉS

Mint azt előzőleg már bemutattuk a sniffeléshez elégséges az, ha a két végpont között olyan eszközön végezzük a lehallgatást, ahol a csomag átmegy.

Mit is jelent ez?

IP alapú hálózatok kommunikációja, a kommunikációs végpontok közötti csomag utak felderítése traceroute segítségével.

Példa a traceroute útvonal felderítésre:

```
1  30 ms   20 ms  30 ms loopback-0.izidor.gw.tvnet.hu [195.38.98.64]
2  30 ms   30 ms  20 ms bvi6.HardCore.gw.tvnet.hu [195.38.98.33]
3  20 ms   30 ms  20 ms bix-ge.adatpark.hu [193.188.137.64]
4  20 ms   30 ms  30 ms origo.matav.hu [195.228.240.145]
```

5.1. Gyakorlati példák 1.a

telnet protokol

Egy hagyományos telnet klienssel történő bekapcsolódás:

```
backup:~# telnet 10.0.0.102 23
Trying 10.0.0.102...
Connected to 10.0.0.102.
Escape character is '^]'.
Debian GNU/Linux testing/unstable omen
omen login: csibi
Password:
csibi@omen:~$
```

5.2. Gyakorlati példák 1.b

telnet protokol

Ami eközben a hálózaton zajlik:

```
backup:~/s# hextype 10.0.0.1.1374-10.0.0.102.23
*** File: 10.0.0.1.1374-10.0.0.102.23
00000000 : FF FB 18 FF FB 20 FF FC-23 FF FB 27 FF FA 20 00 : ˙ű.˙ű ˙ü#˙ú'˙ú .
00000001 : 33 38 34 30 30 2C 33 38-34 30 30 FF F0 FF FA 27 : 38400,38400˙đ˙ú'
00000002 : 00 FF F0 FF FA 18 00 73-63 72 65 65 6E FF F0 FF : .˙đ˙ú..screen˙đ˙
00000003 : FD 03 FF FC 01 FF FB 1F-FF FA 1F 00 50 00 18 FF : ý.˙ü.˙ű.˙ú..P..˙
00000004 : F0 FF FD 05 FF FB 21 FF-FD 01 63 73 69 62 69 0D : đ˙ý.˙ű!˙ý.csibi.
00000005 : 00 63 73 69 62 69 0D 00-                        : .csibi..
```

Látható a telnet protokoll fejléce, a terminál információk és a felhasználói név, jelszó

5.3. Gyakorlati példák 2.a

FTP protokoll

Egy hagyományos ftp klienssel történő bekapcsolódás:

```
backup:~# ftp 10.0.0.102
Connected to 10.0.0.102.
220 ProFTPD 1.2.4 Server (Debian) [omen]
Name (10.0.0.102:root): csibi
331 Password required for csibi.
Password:
230 User csibi logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

5.4. Gyakorlati példák 2.b

FTP protokoll

Ami eközben a hálózaton zajlik:

```
backup:~/s# less 10.0.0.1.1384-10.0.0.102.21
USER csibi
PASS csibi
SYST
```

Látható az FTP protokoll teljesen plaintext adatforgalma, ahol átadásra kerül a felhasználói név és a jelszó.

5.5. Nem hálózati jellegű sniffelés, alkalmazás monitozorás

A módszer csak kliens, vagy szerver oldalon érhető el, semmilyen hálózati hozzáférés nem szükséges hozzá.

Az adott operációs rendszer folyamatkövetési „trace” megoldásain alapszik. Legtöbb esetben privilegizált (root, administrator) jogosultság kell hozzá, ennél fogva létjogosultsága kicsi, de fontos.

Felhasználási területe: egy adott gépről tovább lépő felhasználók azonosítóinak, jelszavainak megszerzése.

Működik titkosított alkalmazások esetén is.

5.6. Alkalmazás monitozorás - példa

ssh kliens alkalmazás felhasználása azonosító és jelszó lopásra

Ami az ssh kliensben látszik:

```
execve("/usr/bin/ssh", ["ssh", "-l", "csibi", "10.0.0.102"], [/* 13
vars */]) =
0
uname({sys="Linux", node="backup", ...}) = 0
[…]
open("/dev/tty", O_RDWR|O_LARGEFILE)    = 4
rt_sigprocmask(SIG_BLOCK, [INT TSTP], [], 8) = 0
ioctl(4, SNDCTL_TMR_TIMEBASE, {B38400 opost isig icanon echo ...}) = 0
ioctl(4, SNDCTL_TMR_CONTINUE, {B38400 opost isig icanon -echo ...}) =
0
write(4, "csibi@10.0.0.102\'s password: ", 29) = 29
read(4, "c", 1)          = 1
read(4, "s", 1)          = 1
read(4, "i", 1)          = 1
read(4, "b", 1)          = 1
read(4, "i", 1)          = 1
read(4, "\n", 1)         = 1
write(4, "\n", 1)        = 1
ioctl(4, SNDCTL_TMR_CONTINUE, {B38400 opost isig icanon echo ...}) = 0
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
```

6. CSOMAG LEHALLGATÁS FELDERÍTÉSE

6.1. PING metódus

Ha a sniffer program által használt tcpstack normál, akkor használható ez a módszer. Küldeni kell egy ICMP Echo request (ping) kérelmet a hálózat minden IP-jére, de olyan formán hogy a címzett MAC addresse ne egyezzen meg a valódi MAC adressével. Normál esetben senki nem fog válaszolni a kérésekre mivel az általunk használt kliens MAC addresse nem az eredeti ezért el fogja dobni a csomagokat, hiszen nem neki címződött az. Viszont a snifferrel ellátott gép válaszolni fog a „promiscuous mode” miatt.

6.2. ARP metódus

A módszer lényegében azonos az PING metódushoz, de ez a módszer működik módosított tcp stackeknél is. A feladat küldeni egy ARP kérelmet egy nem broadcast címre, erre normál esetben senki nem fog válaszolni mivel a hálókártyák eldobják a kérelmet hiszen az nem nekik szól. Viszont a promiscuous módba kapcsolt hálózati interfészek válaszolni fognak rá, hiszen ők megkapja a kérelmet.

6.3. DNS metódus

A módszer olyankor alkalmazható, ha a sniffer programban aktivizálva lett az automatikus DNS visszafejtési opció. Ilyenkor a sniffer program minden új IP-nek megkísérli visszafejteni a host nevét. A megoldás lényege hogy a gépünkről kapcsolatot kezdeményezünk egy idegen IP-re, majd eközben sniffelünk promiscuous módban minden 53-as (dns) portra történő kapcsolódási kísérletet. Majd kielemezzük, hogy volt-e olyan kapcsolat, amely az általunk előállított idegen IP-t tartalmazza, ha volt ilyen akkor az adott gépen minden bizonnyal fut valamilyen sniffer alkalmazás.

6.4. Source-route metódus

A módszer lényege, hogy készítünk egy ping csomagot, melyben be kell kapcsolni a source route opciót, mely egy másik hálózatban található gépre mutat. Ideális esetben az ilyen csomagra nem jöhet soha válasz, hiszen a saját hálózati szegmensünk határain túlra úgysem működne a source-route. Ha azonban kapunk választ akkor szinte biztos, hogy a kérdéses hálózatban, vagy a hálózatok között sniffer fut. A sniffer szegmentális elhelyezkedését meg lehet állapítani a visszakapott válasz TTL mezőjéből.

6.5. Decoy metódus

Ellentétben a ping és ARP metódusokkal, melyek csak lokális hálózaton működnek; a Decoy módszer bárhol alkalmazható. A módszert nevezik még „mézescsupornak” is. A feladat létrehozni egy gépet, melyen elhelyezünk különböző felhasználókat, melyeknek az adott gépen nincs semmilyen jogosultsága. Majd a vizsgált hálózatokból továbbítunk telnet, ftp, pop3,stb. belépéseket az adott gépre. Ezek után arra kell várni, hogy történik-e az adott gépre belépés, ha igen akkor a vizsgált hálózatban minden bizonnyal sniffer fut, amelyet ráadásul biztosan rossz céllal futtatnak. A módszer egyértelműen bizonyítja a sniffer jelenlétét, de a sniffelés és belépés közötti idő nem meghatározható.

6.6. Host metódus

Ha egy hacker betör egy gépre azzal a szándékkal, hogy onnan adatokat lopjon, akkor nagy valószínűséggel futtatni fog ott egy sniffer programot, mellyel további jelszavakat próbál gyűjteni. Ilyen az operációs rendszerre jellemző paranccsal (ifconfig –a, ipconfig, stb.) le kell ellenőrizni, hogy bármelyik interfész promiscuous módban van-e, ha igen, akkor nagy valószínűséggel fut ilyen jellegű program a gépen és érdemes kivizsgálni az esetet.

6.7. Lappangási metódus

A módszer olyankor alkalmazható, ha a sniffer alkalmazást futtató gépet a támadó megfelelően felkonfigurálta, így semmilyen előzetes vizsgálaton nem bukott el a gép (ICMP, ARP, stb.).

A módszer csak akkor működőképes, ha a gép promiscuous módban fut és a hálózat nagy áteresztőképességű. Olyan mennyiségű forgalmat kell generálni random cél IP-kre, mely teljesen „betömi" az adott hálózatot és meg kell nézni az egyes gépeket a hálózatban. A gépeken a CPU terheltséget kell figyelni. Ha a vizsgálat ideje alatt az adott gép CPU terheltsége sokkal magasabb mint egyéb esetekben; akkor feltehetően fut rajta valamilyen csomag analizátor program.

6.8. TDR (Time-Domain Reflectometers)

Hardveres packer sniffer kereső eszközök, több ismert módszert használnak kombinálva.

6.9. Csomaglehallgatás felderítő szoftverek:

- AntiSniff

http://www.l0pht.com/antisniff/

- CPM (Check Promiscuous Mode)

ftp://coast.cs.purdue.edu/pub/tools/unix/cpm/

- neped

http://www.apostols.org/projectz/neped/

- sentinel

http://www.packetfactory.net/Projects/sentinel/

- Ifstatus

ifstatus

7. SNIFFELÉS SPECIÁLIS KÖRÜLMÉNYEK KÖZÖTT

7.1. Kábel modem/ DSL,ADSL szegmens sniffelése

Az elsődleges probléma, hogy a kábel modemek a feltöltési és a letöltési streameket két külön asyncronos csatornán továbbítják. A kábel modemeknek van egy „receive-only" csatornája mely egy nagy sebességű (30-mbps, 50-mbps közötti csatorna) és van egy „transmit-only" alacsony sebességű csatornája (rendszerint 1-mbps alatt); viszont a kábelmodem transmit csatornáját nem lehet olvasni.

A legtöbb kábelmodem box rendelkezik egy 10-mbps ethernet csatlakozóval, melyen keresztül a 30-mbps maximalizált sávszélesség csak szűkítve tud átjönni.

Minden kábelmodem eszköz saját MAC-el és rendszerint saját IP-vel is rendelkezik, így ha a gép hálózati interfészét promisuous módba is állítjuk, az nem jelent semmit a kábelmodem miatt.

Broadcast: a különböző alkalmazások broadcast kérései lehetőséges nyújtanak arra, hogy feltérképezd a kábelmodemes szegmens többi gépét. Ilyenek lehetnek a NetBIOS kérelmek, SNMP broadcast kérelmek és a bootp/DHCP kérelmek. Ezek monitorozása révén felismerhető a hálózat elemei.

Átirányítás: mivel sniffelni nagyon nem lehet az ilyen hálózatokban ezért marad a forgalom átirányítás, erre több módszer is van (ARP, ICMP Redirect , ICMP Router Advertisements); a szolgáltató felkészültségétől függ, hogy melyikkel lehet elérni a csomagok átirányítását.

7.2. Wireless, IEEE802.11 (AirPort) sniffelés

A wireless standard tartalmaz egy „spread spectrum" technológiát. Ez a technológia a sniffelés lehetőségének alapja.

A sniffelés fizikai határai : 100m szobában, 300m szabad ég alatt.

Titkosítás: a vezetéknélküli technológiák egységesen a „Wired Equivalent Privacy (WEP)„. A módszer alapja az RC4 titkosítás 40-bit-es kulcsú módszere. A legtöbb browser-nek szintén ez a alapértelmezett titkosítási módszere. Az RC4 ki van terjesztve a 128-bitre is, de az 802.11-es szabvány az exportkorlátozások miatt CSAK a 40 bit-et írja ki. A WEB csak az adatrészeket titkosítja, így a sniffer program képes érzékelni a fizikai adatszinteket és képes előkészíteni a lényegi adatokat a visszafejtésre. A WEP egy „megosztott-kulcs" architektúrát alkalmaz, mely alapvetően egy nagyon rossz tervezés. Itt a tényleges kulcs rendszerint kisebb mint a 40 bit így a visszafejtése nagyságrendekkel csökkenhet. Összegezve a titkosított adat visszafejtése bonyolult, de nem lehetetlen. Ma már léteznek olyan célhardverek amely reális időn belül képesek ilyen titkosítást visszafejteni.

7.3. Sniffelés switchelt hálózaton.

Alapvető tény, hogy switchelt hálózaton nem lehet sniffelni, hiszen a switchelt hálózatnak pont az a lényege, hogy a switch az egyes portok között csak az adott portra címzett csomagokat továbbítja, így nem hiába állítjuk promiscuous módba a hálókártyát akkor sem fogjuk megkapni a többi gépnek címzett csomagokat.

Ennek ellenére természetesen ez a módszer is kijátszható az esetek nagy többségében, bár léteznek olyan switchek amelyeket nem lehet sniffelni. (port security)

Switchelt hálózat sniffelésének alapja az a tény, hogy a switchnek is tudnia kell, hogy melyik porton milyen gépek találhatók, ezt pedig egy táblázatban tárolja, mely táblázat egy kaszkád verem elvű tároló egység, melynek lényege hogy a legelőször felvett elem esik ki legelőször. Így, ha megfelelő mennyiségű szemét adat kerül a táblázatba, akkor a switch nem tudja, hogy a cél melyik porton található ezért rendszerint kiküldi minden portra, így mi is megkapjuk.

A fenti módszer elég elavult és számos módszer van még amelyekkel át lehet venni egy másik gép forgalmát, forgalmának részeit egy-egy adott géptől.

Címszavakban a módszerek: ARP redirect, ICMP redirect, ICMP Router Advertisements, tanuló switcheknél jól jön a MAC hamisítás, vagy managelhető switcheknél a monitor port átkonfigurálása.

8. HOGYAN LEGYÜNK „LEHALLGATÁS BIZTOSAK”

8.1. Idegen alkalmazás

Amennyiben hálózatunkba új elemet helyezünk el, melyről nem tudhatjuk, hogy milyen protokollokon kommunikál javasolt megvizsgálni azt lehallgathatóság szempontjából.

8.2. Saját fejlesztésű alkalmazás

Fontos, hogyha olyan alkalmazást fejlesztünk amelynek van hálózati szintje, akkor végezzünk előzetes tervezést. A tervezés fő momentumai: milyen biztonsági besorolású információk közlekednek a hálózaton, milyen folyamatokat befolyásolnak a kommunikációk, milyen jogosultsági szinten fut a szerver és a kliensek.

Ezek az információk alapján kell meghatározni, hogy milyen szintű titkosítási, hitelesítési megoldásokat érdemes alkalmazni. Ha a kommunikáción belül értelmezhetőek biztonsági szintek, akkor javasolt ezeket szintén szétválasztva alkalmazni a kommunikációban.

Alapvető szabály, hogy bármennyire is lényegtelen információk is továbbítódnak az adatcsatornán legalább egy szimpla SSL-t húzzunk a kommunikációra. Számos ingyenes SSL implementáció létezik. A leggyakrabban használt az OpenSSL, melyet számos platformra implementáltak és illesztése bármilyen alkalmazáshoz pofon egyszerű.

9. BIBLIOGRÁFIA

Robert Graham's Sniffing FAQ:
http://www.robertgraham.com/pubs/sniffing-faq.html

Eszközök sniffelhetősége, osztályzások:
http://www.nwo.net/osall/Methodology/Novice/Sniffer_FAQ/sniffer_faq.html

10. EGYÉB

10.1. Jelen dokumentum közlése

Az információk minőségéről

Jelen dokumentum a publicitása miatt nem tartalmaz mindenre kiterjedő részletes információkat. A megoldások egy része a SaveAs Kft. saját know-howja, fejlesztése, stb., így ezen információkat a SaveAs Kft. bizalmasnak tekinti és ezek közlésére nem ad módot.

10.2. CopyRight

Kizárólagos jogok

Jelen dokumentáció a SaveAs Kft. szellemi terméke és kizárólagos tulajdona.

Hasznosítás és többszörözés

Jelen dokumentációt az olvasó üzletszerzésre nem hasznosíthatja. A dokumentum nem módosítható, azonban változtatás nélkül szabadon terjeszthető.

Nyilvánossághoz való közvetítés és idézés

Jelen dokumentáció egészének vagy részeinek médiában vagy bárhol máshol való felhasználása kizárólag a SaveAs Kft. nevének megemlítésével tehető az alábbi módokon:

Televízió és rádió: a SaveAs Kft. nevének megemlítésével és/vagy – televízió esetén - kiírásával.

Újság: a SaveAs Kft. nevének és weblapjának elérhetőségének kiírásával (http://www.saveas.hu).

Digitális média: a SaveAs Kft. nevének és weblapjának elérhetőségének kiírásával (http://www.saveas.hu) és utóbbinak kattintható belinkelésével.

Oktatás

Oktatási célra a dokumentáció szabadon felhasználható.

Minden más esetben

a SaveAs Kft. írásbeli engedélye szükséges.