10. *fejezet- Tartalom*

10 *A Denial of Service támadás*

A *DoS-(Denial of Service* -- szolgáltatás megtagadó) támadások az internet egyik legnagyobb veszélyforrásává váltak az idők során. Egy ilyen támadásnál számítógépeket rohannak le az interneten, és úgy lefagyasztják, hogy az egy ideig nem is tudja újrakezdeni a működését. A DoS-támadások ugyanúgy érintik az internet-felhasználókat, mint a szervereket, például a webszervereket. Az egyik legismertebb támadást 2000 februárjában, két napon belül indították a *Yahoo,* az *eBay,* a CNN és néhány más nagyobb portál ellen a hálón. A rendszerek kiesése következtében fellépő kár mintegy *100 millió dollárra* rúgott. A DoS-támadások az operációs rendszerek, programok és protokollok hibáit használják ki, ami azt jelenti, hogy ezeknek a támadásoknak különböző fajtái vannak. Az eredmény azonban mindig ugyanaz: a megtámadott számítógép felmondja a szolgálatot.

DoS-támadásokat többnyire akkor hajtanak végre, ha a támadó nem talál más utat, hogy a rendszert lerohanja, vagy ha éppen az a célja, hogy a rendszert egy időre lebénítsa. A DoS-támadások célzott végrehajtásának másik oka lehet például, hogy egy rendszert újraindításra kényszerítsenek valamilyen változtatás érvénybe léptetése érdekében (jelszó: trójai). Kedvelt célok azok a felhasználók is, akik game-szervereken vagy IRC-szervereken találhatók.

A különböző támadásokhoz egész sor eszköz áll a támadók rendelkezésére, amelyeknek többnyire jól kezelhető, grafikus felületük van, így a támadónak még alaposabb technikai ismeretekkel sem kell rendelkeznie a használatukhoz.

10.1 Az IP-spoofing mint előfeltétel

Az *IP-spoofing* egy támadási eljárás, amelynél hamis IP-számot használnak, hogy hamis identitást színleljenek a megtámadott IT-rendszer felé.

Az IP-spoofing, amelynél a csomag feladójának a címét megváltoztatják, sok DoS-támadás alapját képzi. Vagy már a támadást is ez teszi lehetővé, vagy arra szolgál, hogy a támadó nyomait eltüntessék, és megakadályozzák az azonosítását. Így a támadót, aki két napig bombázta a Yahoo-t és társait, csak a hencegése alapján kapták el egy idevágó chatszobában.

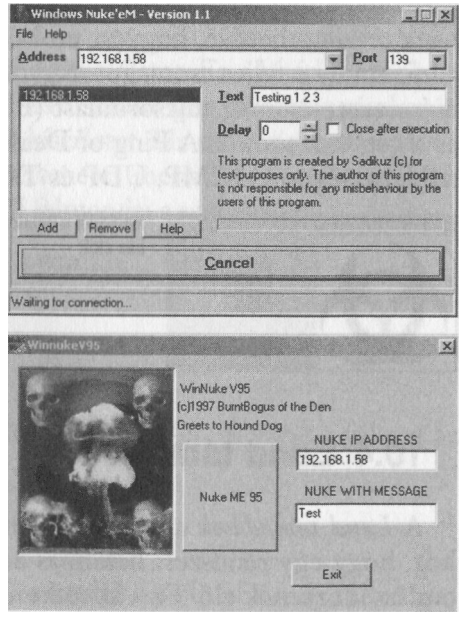
1998-ban létrejött egy védelmi szervezet, amely lehetetlenné teszi hamisított IP-csomagok internetre küldését a csatlakoztatott hálózatüzemeltetőknél. Sajnos, ez csak egy behatárolt megoldás, mert csak a szervezethez kapcsolódó rendszerekből érkező támadásokat akadályozza meg.

10.2 Out-of-Band csomagok - a „nuken"

A legismertebb DoS-támadások közé tartozik a *miken* vagy az *Out-of-Band (OOB)* csomagok küldése. Az OOB a TCP/IP egyik tulajdonsága, és ezzel a protokollal továbbítódik. Megengedi az adatok átvitelét a normál sorrenden kívül, és - többek között - Telnet session-ökhöz használják.

Az Out of Band csomagok felhasználását a DoS-támadásokhoz a *Microsoft* egy hibás *NetBEUI implementációja* tette lehetővé. Ha a 135. és a 139. portok egy számukra nem értelmezhető karaktersort kapnak, a rendszer összeomlik. A Microsoft felismerte ezt a hibát, és mind a Windows 98/98SE/ME-t, mind a 2000-t ellenállóvá tette e támadások ellen. Ezért az Out of Band csomagokat az olyan rendszerek megtámadásához használják, mint például a *WinGates.*

A WinGates 4.01-t például így lehetne megtámadni: 100 kapcsolatot állítanak elő a WinGates-hez, és ezeken egyenként körülbelül 40000 karaktert küldenek. A WinGates-szerver feltételezi, hogy minden



Kettő a legismertebb nukerek közül

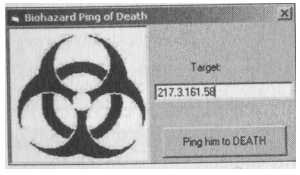
kapcsolat fennmarad, és az adattömeg addig halmozódik, amíg el nem használja a szerver pufferét. Ha most a rendszergazda megpróbál belépni, *out of buffer* hibaüzenetet kap.

10.3 Large Packet-támadások avagy a Ping of Death

A Denial of Service támadások különösen végzetes fajtája a *Ping of Death*. Ez utóbbinak semmi köze a tulajdonképpeni ping-parancshoz, amelyről ebben a fejezetben még szó lesz.

Az Internet Protokoll headerrel (fejléccel) együtt pontosan 65535 bájtot csomagol egyetlen csomagba, az Ethernet-csomagok pedig csak 1500 bájtosak. Az ennél nagyobb csomagokat fragmentálja, vagyis feldarabolja, hogy egyszerűbb legyen az átvitelük, és aztán újra reassemblálja (összerakja) őket. Mindez azért történik, hogy az adatok át tudjanak futni a különböző hálózati rétegeken.

Minden csomagtöredék tartalmaz egy *offset értéket* és egy azonosítási számot. Az első csomagban még egy *TCP-header* is található, valamint a *portszám,* amely meghatározza, hogy milyen csomagról van szó. Ezek a tények teszik lehetővé, hogy az utolsó töredéknek olyan offset értéket lehet adni, amely a teljes csomagot nagyobbnak mutatja 65535 bájtnál. Ez a túlméretezett csomag túlcsordulást (Buffer Overflow-t) okoz a rendszerben, és a gép összeomlik. A Ping of Death támadások a következő protokolloknál lehetségesek: ICMP, UDP és TCP.



Röviddel a halálos lökés előtt

10.4 Land támadások

A *Land támadások* a TCP-implementáció egy hibáját használják ki ahhoz, hogy egy rendszert hatalmas adatfolyammal terheljenek, majd összeomlást idézzenek elő. Ez a következőképpen történik.

Mikor egy számítógép kapcsolatot próbál felépíteni egy másikkal, akkor *speciális IP-csomagokat* küld, amelyekkel bejelenti a kapcsolatot. Ezeket *SYN-csomagoknak* is nevezik. A címzett reagál erre, és válaszul ACK-csomagot (ACK = Acknowledgement = a fogadás nyugtázása) küld. Ezt a folyamatot *Three Way Handshake-nek* is nevezik. Aki viszont Land támadást hajt végre, a protokoll-implementáció említett hibáját kihasználva, hamisított feladóval küldi a SYN-csomagokat egy szerverre - a feladó címe megegyezik a címzettel. A szerver minden SYN-csomagra ACK-csomaggal válaszol, de ezt a csomagot most egy saját nyitott portjára fogja küldeni, ahol a sok IP-stack egyfajta túlcsordulást idéz elő, és megbénítja az áldozat rendszerét.

A támadásnak ezt a fajtáját az elkészült bugfixekkel ma már a legtöbb operációs rendszer visszaveri.

10.5 TCP-Syn-Flooding

Mint ahogy a Land támadásoknál már leírtuk, ha két számítógép között TCP/IP-n keresztül jön létre kapcsolat, a résztvevők először egy *Three Way Handshake-et* váltanak. A *TCP-Syn-Flodding* támadásnál a támadó először hamis feladóval nagy számú SYN-csomagot, vagyis „Beszélni akarok veled" üzenetet küld a hostra. A host ezt megpróbálja egy „OK, kész vagyok" ACK-válaszcsomaggal nyugtázni, és előállítani a kapcsolatot. Ez a kísérlet azonban, a nemlétező feladó miatt, sikertelen lesz, és a számítógép bizonyos várakozási idő után eredménytelennek nyilvánítja a kísérletet. Ha ezt a várakozási időt a támadó arra használja, hogy a hostot rettenetes mennyiségű további SYN-csomaggal bombázza, az rövid időn belül felmondja a szolgálatot.

íme, egy ilyen támadás lefolyásának a sémája.

- A támadó elküldi a SYN 1-et.
- A host válaszol a SYN 1-re, elküldi az ACK 1-et, és várja a választ.
- A támadó elküldi a SYN 2-t.
- A host válaszol a SYN 2-re, elküldi az ACK 2-ét, és várja a választ az ACK 1-re és 2-re.
- A támadó elküldi a SYN 3-at.
- És így tovább.

Ezek ellen a támadások ellen is régóta létezik már bugfix.

10.6 Ping-Flodding

A pingeket az interneten és a hálózatokban használják, hogy megállapítsák egy host elérhetőségét. Megpingelünk egy hostot, és ha elérhető, visszhangszerű választ ad. Ezt használják ki a támadók a Ping-Floddingnál. Pingekkel bombázzák a célt, a host pedig valamennyire megpróbál válaszolni. Ha az ismétlés elég gyakori, a host nem tud több kérdésre válaszolni. Ráadásul a ping-flodding támadásokat az áldozat csak akkor fogja észrevenni, ha a szolgáltatója a forgalom szerint számol el.

10.7 Smurf

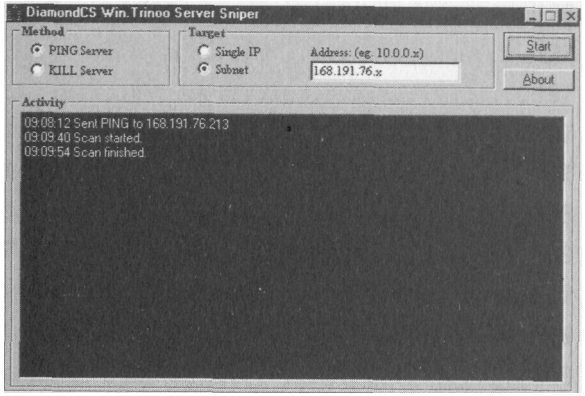
A *Smurf-nél* a támadó egy hálózat broadcast címére küld egy pinget manipulált feladócímmel, amelyre minden, a broadcast cím mögötti számítógép válaszol. Ez bizony rengeteg választ jelent. A megváltoztatott feladócímek, az áldozatéi, azt eredményezik, hogy minden választ az áldozat kap meg. Ha ilyen módon másodpercenként 1000 pinget küldenek 1000 különböző számítógépre, az áldozat több mint egymillió választ kap. Az érintett rendszer a bemenő adatok terhe alatt szó szerint összeomlik. Az ilyen támadások után többnyire teljesen le kell venni a szervert a hálózatról.

Smurffel akár nagyon kis átviteli kapacitással rendelkező támadók (modem- vagy ISDN-csatlakozás) is térdre tudnak kényszeríteni nagy átviteli sávszélességgel rendelkező áldozatokat.

10.8 DDoS- Distributed Denial of Service támadások

A DDoS-nál (DDoS-támadás = elosztott szolgáltatás megtagadó támadás) még a tulajdonképpeni roham előtt szerez a támadó elérést néhány másik rendszerre, és ezeket arra használja, hogy az áldozatát nagy mennyiségű adatcsomaggal szembesítse. Az előkészítés abból áll, hogy a támadó a lehető legtöbb olyan rendszert megtalálja, amelyeken biztosítani tudja magának a rendszergazdai jogokat, hogy fel tudja tölteni a scripteket a támadáshoz. Ehhez a támadó hibás rendszereket keres szkenneléssel (közelebbit lásd a szkennelésről szóló fejezetben). Ezeken a rendszereken trójaiakat helyez el, hogy távirányítani tudja a számítógépeket. (A trójaikról a 4. fejezetben írtunk.) Ha elegendő kiszolgálót talált, ezeket feltölti scriptekkel vagy programokkal, s az áldozatot csomagok áradatával önti el, amitől az összeomlik. A 2000. februári híres DDoS támadások óta állandóan növekszik az ilyen jellegű támadásokra alkalmas programok száma a *Yahoo,* az *eBay* és társai ellen.

Előkészület egy DDoS támadásra



10.9 Védelem a DoS-támadások ellen

A normál felhasználó számítógépe nemcsak áldozata lehet a DoS-támadásoknak, hanem arra is használhatják a támadók, hogy rajta keresztül hajtsák végre más rendszerek ellen a támadásokat. A scripteket, illetve a programokat többnyire trójaiak segítségével telepítik a rendszerekre, ezért is elengedhetetlen, hogy *mindig legyen aktuális vírusvizsgáló a gépünkön*.

A DoS-támadások ellen *a jól konfigurált tűzfalak* is védelmet kínálnak. A segítségükkel el lehet kapni a módosított csomagokat, és meg lehet akadályozni, hogy sor kerüljön a további feldolgozásukra.

Legyen az szerver vagy normál felhasználó - minden esetben érvényes, hogy mindig tájékozódni kell a mindenkori operációs rendszer biztonságot érintő frissítéseiről. A gyártók előbb vagy utóbb felfedezik az operációs rendszerekben és a szerverszoftverekben a biztonsági szempontból gyenge pontokat, és rövid idő múlva frissítést kínálnak hozzájuk. Hogy a gyenge pontok dolgában mindig képben legyünk, érdemes előfizetni a *Computer Emergency Response Teams (CERT)* levelezőlistájára **http://www.cert.org** és a gyártóéra. Ezek azonnal tájékoztatnak az újabb gyenge pontok felfedezéséről, és beszerzési forrást kínálnak a megfelelő frissítésekhez.