Dagens företag har ett bra skydd mot överbelastningsattacker

Examensarbete inom datavetenskap
10 poäng, C-nivå, våren 2004

Författare: Mikael Granberg
Mattias Harneman

Handledare: Bo-Krister Vesterlund
Examinator: Gouhua Bai
Förord

Vi skulle vilja tacka nedanstående personer, som har gjort det möjligt för oss att genomföra denna uppsats och hjälpt oss under arbetets gång.

Vår examinator:
Gouhua Bai

Vår handledare:
Bo-Krister Vesterlund

Personer som har deltagit och ställt upp för vår skull i intervjuer:

Björn Mattson (Datorenheten Blekinge Tekniska Högskola)
Mattias Andersson (JME Data AB)
Joacim Åstedt (LunarWorks AB)
Anders Johansson (Enjoy)
Gerth Malmevik (Ginza)
Abstract

Today's society is more vulnerable than one occasionally expects. Denial of service attacks is aimed against an explicit network, with the intent of making its services unavailable to legitimate users. This is something that happens every day against corporations around the world, and not the least in Sweden. Lately media has noticed this problem, since it is becoming more and more frequent amongst corporations.

The purpose of this thesis is partly to gain a better understanding if denial of service attacks are of any priority or not, but also to get the corporations focus when it comes to which protections that are available against this sorts of assaults, and to make them to actually think about what kinds of treats that are really out there.

Our aim in this thesis is to find out which kinds of protections corporations in Sweden is using at the moment, but also which they can and ought to be using. To reach this aim of ours, we conducted interviews with corporations that are operating a large part of their sales, or provides a service, over the Internet.

This has made that we have come to conclude that the corporations admittedly have protection against denial of service attacks and makes use of it themselves, but that they also should have a look at other kinds of protections that are available and might function even better for them. There is after all good ways to protect yourself against these types of attacks, but you have to know how they function and to take advantage of them in the right way.

We hope, and believe, that this work of ours, will be of some help for the corporations in the future to easier resist denial of service attacks, and it is our expectation that this thesis will come to use and serve its purpose.
Sammanfattning

Dagen samhälle är sårbarare än man ibland kan ana. Överbelastningsattacker är attacker mot ett specifikt nätverk, och syftet är att göra dess tjänster otillgängliga för legitima användare. Detta är något som sker varje dag mot företag runtom i världen, och inte minst i Sverige. Media har på senare tid uppmärksammat problemet sedan det blivit allt vanligare och vanligare bland företagen.

Syftet med detta arbete är dels att få bättre förståelse om överbelastningsattacker är något som prioriteras eller inte, men även att få företagen uppmärksammade på vilka olika skydd som finns att tillgå mot överbelastningsattacker, samt att vi vill få företagen att verkligen tänka på vilka hot som finns där ute.

Vårt mål med denna uppsats är att ta reda på vilka befintliga skydd företag i Sverige använder sig utav för tillfället samt vilka skydd de kan och bör använda sig utav. För att nå detta mål har vi genomfört kvalitativa intervjuer med företag som bedriver en stor del av sin försäljning, eller tillhandahållande av tjänster, över Internet.

Detta har gjort att vi kommit fram till att företagen visserligen visst har skydd mot överbelastningsattacker och använder sig utav dem, men bör också se till vilka andra skydd som finns tillgängliga för dem och kan fungera bättre för just dem. Det finns som sagt bra skydd mot överbelastningsattacker, men det gäller att veta hur de fungerar och att använda dem på rätt sätt för att kunna utnyttja dem ordentligt.

Vi tror, och hoppas, att detta arbete kommer att kunna hjälpa företagen i framtiden att lättare kunna stå emot överbelastningsattacker, och det är våran förhoppning att denna uppsats kommer att komma till nytta och tjäna sitt syfte.
Innehållsförteckning

1. INLEDNING .................................................................................................................................1
   1.1 BAKGRUND ....................................................................................................................................1
   1.2 PROBLEM/FRÅGESTÄLLNING ........................................................................................................2
   1.3 SYFTE .............................................................................................................................................2
   1.4 MÅLGRUPP ....................................................................................................................................2
   1.5 AVGRÄNSNINGAR ..........................................................................................................................3
   1.6 MÅL ...............................................................................................................................................3
2. TEORETISK BAKGRUND ............................................................................................................4
   2.1 BANDBREDDSFÖRBRUKNING ........................................................................................................6
      2.1.1 ICMP-strömmar ....................................................................................................................7
      2.1.2 UDP-strömmar ......................................................................................................................7
      2.1.3 Smurf .....................................................................................................................................7
      2.1.4 Fraggle ..................................................................................................................................7
      2.1.5 Slammer ....................................................................................................................................7
      2.1.6 Stacheldraht – attackverktyg .................................................................................................8
      2.1.7 Trinity – attackverktyg ..........................................................................................................8
   2.2 UTSVÄLTNING ................................................................................................................................9
      2.2.1 SYN-strömmar .......................................................................................................................9
      2.2.2 E-mailbombning ....................................................................................................................9
      2.2.3 Stream – attackprogram ........................................................................................................9
   2.3 PROGRAMMERINGSFEL .............................................................................................................10
      2.3.1 Teardrop ..................................................................................................................................10
      2.3.2 Ping of Death ..........................................................................................................................10
      2.3.3 Routnings- och DNS-angrepp ...............................................................................................10
   2.4 FÖRSVAR MOT ÖVERBELASTNINGSATTACKER .....................................................................11
      2.4.1 Förebygga ..............................................................................................................................11
      2.4.2 Skydda ....................................................................................................................................12
      2.4.3 Upptäcka ...............................................................................................................................19
      2.4.4 Reagera ....................................................................................................................................19
   2.5 FRAMTIDA FÖRSVAR MOT ÖVERBELASTNINGSATTACKER ......................................................21
## 3. METOD

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 INTERVJU</td>
<td>22</td>
</tr>
<tr>
<td>3.2 FRÅGEFORMULÄR</td>
<td>23</td>
</tr>
<tr>
<td>3.2.1 Tänkbara problem</td>
<td>24</td>
</tr>
<tr>
<td>3.3 INTERVJUER – FÖRETAG</td>
<td>25</td>
</tr>
<tr>
<td>3.3.1 Tänkbara problem</td>
<td>25</td>
</tr>
<tr>
<td>3.4 LITTERATUR</td>
<td>26</td>
</tr>
<tr>
<td>3.5 INTERNET</td>
<td>26</td>
</tr>
</tbody>
</table>

## 4 RESULTAT

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 HUR KAN FÖRETAGEN SKYDDA SIG MOT ÖVERBELASTNINGSATTACKER?</td>
<td>27</td>
</tr>
<tr>
<td>4.2 HAR DAGENS FÖRETAG BRA SKYDD MOT ÖVERBELASTNINGSATTACKER?</td>
<td>30</td>
</tr>
<tr>
<td>4.3 SAMMANFATTNING AV RESULTATET</td>
<td>33</td>
</tr>
</tbody>
</table>

## 5. DISKUSSION

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
</tr>
</tbody>
</table>

## 6. SLUTSATSER

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
</tr>
</tbody>
</table>

## 7. REFERENSER

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 BÖCKER</td>
<td>37</td>
</tr>
<tr>
<td>7.2 ARTIKLAR</td>
<td>37</td>
</tr>
<tr>
<td>7.3 INTERNET</td>
<td>37</td>
</tr>
<tr>
<td>7.4 KÄLLHÅNVISNINGAR</td>
<td>38</td>
</tr>
</tbody>
</table>

APPENDIX I – INTERVJUFRÅGOR

APPENDIX II - FRÅGEFORMULÄR

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRÅGEFORMULÄR (SÄLJANDE FÖRETAG)</td>
<td>1</td>
</tr>
<tr>
<td>FRÅGEFORMULÄR (TJÄNSTEFÖRETAG)</td>
<td>2</td>
</tr>
</tbody>
</table>

APPENDIX III - INTERVJUSVAR FÖRETAG

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>JME DATA</td>
<td>1</td>
</tr>
<tr>
<td>LUNARWORKS</td>
<td>2</td>
</tr>
<tr>
<td>ENJOY</td>
<td>4</td>
</tr>
<tr>
<td>GINZA</td>
<td>5</td>
</tr>
</tbody>
</table>
1. Inledning

1.1 Bakgrund

Överbelastningsattacker är attacker, organiserade eller ej, mot ett helt nätverk, en specifik webservrar eller andra resurser, och har som mål att slå ut dem och göra så att dess tjänster inte längre är tillgängliga för legitima användare. Man har mer och mer börjat höra om dessa attacker i media och då är det ofta större företag som bedriver någon form av e-handel, eller tillhandahåller tjänster med större delen av deras försäljning eller utbud av tjänster på nätet.

Det som har gjort överbelastningsattacker så vanliga är att i princip vem som helst med lite datorvana kan utföra dessa attacker, med hjälp utav lite programvara, och kan då slå ut system och nätverk med stor kapacitet, utan att själv besitta någon större kapacitet.

Vad många former av överbelastningsattackar gör är att den, eller de personer som skall utföra attacken, sprider maskar\textsuperscript{1} eller trojaner till datorer runtomkring i världen och sedan vid en specifik tidpunkt så sätts attacken igång från alla dessa datorer, och blir på så sätt väldigt kraftfull. Detta kallas för en distribuerad överbelastningsattack.

Ägarna till de datorer som är inblandade i en sådan attack vet oftast inte ens om att de deltar, och deras datorer brukar då få benämningen zombies, det vill säga övertagna maskiner som styrs utav en huvuddator.

Syftet med dessa attacker kan vara allt från utpressning av pengar från företagen, eller helt enkelt bara en hämndaktion för en artikel eller ett förfarande man kanske inte gillade.

I en undersökning\textsuperscript{2} gjord 2002 av NHTCU – National Hi-Tech Crime Unit i Storbritannien uppgav 20 % av de intervjuade företagen att de råkat ut för Denial of Service-attacker. Förutom förlorade inkomster då företaget inte kan nås via Internet, skapas naturligtvis dålig publicitet för företaget, vilket gör att det är viktigt att kunna skydda sig mot sådana attacker.

Det må vara 2004 nu, men denna typ av attacker blir bara vanligare och vanligare mot företag runtomkring i världen och även i Sverige.

\textsuperscript{1} En mask är i datorsammanhang ett stycke bakterieartad programvara som sprider sig själv från dator till dator genom att t ex utnyttja befintliga säkerhetshål och felkonfigurerings.

\textsuperscript{2} Från NHTCU's hemsida http://www.nhtcu.org/NHTCU%20NOP%20survey.pdf (sid 4)
1.2 Problem/frågeställning

Det vi vill ta reda på inom ramen för vårt kandidatarbete är vad företag i Sverige egentligen har för skydd mot överbelastningsattacker. Blir de utsatta ofta för sådana attacker? Behövs det överhuvudtaget ett skydd mot överbelastningsattacker?

Med utgång från dessa frågor har vi formulerat följande huvudfråga samt underfråga för att vidareutveckla huvudfrågan:

Huvudfråga:  
- Har dagens företag ett bra skydd mot överbelastningsattacker?

Underfrågor:  
- Hur kan företagen skydda sig mot överbelastningsattacker?

1.3 Syfte

Varför görs då detta kandidatarbete? Det är bland annat för att kunna få en bättre inblick hur svenska företag egentligen fungerar och hur mycket tänker de, och bryr sig om säkerheten i företaget. Är attacker av den typen som vi skriver detta arbete om något som prioriteras eller kommer det någonstans i andrahand?

Vi hoppas i alla fall kunna framföra till företagen, olika skydd för att lättare kunna stå emot överbelastningsattacker och att till en viss del bidra till att företag blir mer uppmärksammade och tänker en gång till på de faktiska hot som finns där ute i och med Internets framfart i världen.

1.4 Målgrupp

De målgrupper vi riktar oss till inom detta kandidatarbete är för det första företag som bedriver någon sorts försäljnings av produkter och använder sig av Internet vid försäljningen av dessa. Detta kan vara alla sorters företag från en datorbutik till bokförsäljare eller en sajt för kommersiell spelverksamhet.

Den andra delen av vår målgrupp är företag som istället för att ha försäljning på Internet, så tillhandahåller de istället gratis tjänster till konsumenterna. Företag inom denna kategori är då allt från företag som sysslar med webbcommunities till dagstidningar.

---

3 Försvenskning av engelskans sida. I media brukar ordet "sajt" eller "webbsajt" få beteckna allt som har med Internet att göra, oavsett om det är en webbplats eller en programvara

4 Webbccommunity är beteckningen för en interaktiv mötesplats på Internet.
1.5 Avgränsningar

Vi kommer endast att inrikta oss på synen på överbelastningsattacker från ett företagsperspektiv och kommer alltså inte att gå in på exempelvis Internetleverantörernas (ISP:s) synvinklar.

Vi kommer dessutom att inrikta oss på företag som bedriver huvuddelen, eller en stor del av deras, antingen försäljning, eller tillhandahållande av tjänster, på nätet.

Inte heller har vi tänkt inrikta oss på de datoranvändare som blir utnyttjade via sådana här attacker, vare sig de är direktinblandade – de som fungerar som mellanhänder vid attackerna, eller de som indirekt påverkas av att det attackerade företagens tjänster är nere och inte går att komma åt för tillfället.

Dock att tänka på som fortsatt arbete till magisteruppsats kan det vara en bra idé att kunna få med fler synsätt, och då använda sig av de ovanstående som vi utelämnar.

1.6 Mål

Som vi tidigare i inledningen har varit inne på, så är målet med den här uppsatsen att ta reda på vad för slags skydd dagens företag i Sverige egentligen har mot överbelastningsattacker, om de har några alls.

Vi vill även ta reda på vad det egentligen finns för skydd för företagen att tillgå idag.

Detta är alltså vad vi hoppas på att kunna få fram i Resultat delen samt att kunna diskutera den vidare som måluppfyllelse i Diskussionen av arbetet.
2. Teoretisk bakgrund

Många överbelastningsattacker har på senare tid fått stor uppmärksamhet i media. Här visas ett urval av dessa.

"I februari 2000 attackerades ett flertal stora företag av överbelastningsattacker. Bara attacken mot Yahoo, CNN och Ebay beräknades kosta runt en miljard dollar".


Ovanstående artiklar kan få en att tro att överbelastningsattacker endast utförs på grund av ekonomiska intressen, men ett flertal andra artiklar vittnar om att dessa attacker utförs även av andra orsaker.

I mars 2003 stämde SCO Group IBM på 1 miljard dollar, vilket senare ökades till 3 miljarder dollar. SCO ansåg att de hade rättigheten till vitala delar av Linux källkod. Anhängare till öppen källkod sades vara ansvariga för att, som följd till denna stämning attackerat och tagit ner SCO:s servrar under en längre period med överbelastningsattacker.


---

5 ISPs and Denial of Service Attacks, K. Narayanaswamy, Ph.D, 2002 (Sida 2)
6 http://news.bbc.co.uk/1/hi/technology/3549883.stm
7 http://security.itworld.com/4339/040128gamblingsites/page_1.html
Vad är egentligen överbelastningsattacker? Den översättning vi har använt oss av kan vara lite missvisande i vissa fall. Denial of Service (DoS) är den engelska benämningen för överbelastningsattacker. Enligt Paginas IT-ordbok benämns Denial of Service också på svenska som översvämnings- och blockeringsattacker\(^{10}\).

CERT Coordination Center\(^{11}\) beskriver DoS som attacker som har som primärt mål att neka användare access till en särskild resurs. De delar upp attackerarna i tre olika typer:

- Konsumtion av knappa resurser
- Förrärande eller modifiering av konfigureringsinformation
- Fysisk förstörelse eller modifiering av nätverkskomponenter

Enligt McClure m.fl.\(^{12}\) finns det fyra olika typer av överbelastningsangrepp:

- Bandbreddsförbrukning
- Utsvältning
- Programmeringsfel
- Routnings- och DNS-angrepp


För att återvända till CERT :s tre typer av attacker:

Första punken - konsumtion av knappa resurser syftar till att en dator eller ett nätverk behöver vissa resurser för att fungera som de ska. Nätverksbandbredd, minne, interna datastrukturer, diskutrymme, CPU-tid, access till andra datorer och nätverk och vissa miljöresurser såsom el, kall luft med mera.

Oftast när man hör talas om överbelastningsattacker idag så gäller det attacker mot nätverksbandbredd genom bland annat skicka mängder (strömmar) med paket till en dator eller ett nätverk vilket gör att lite eller ingen legitim trafik kommer fram. Detta kan ske från en, eller ett nätverk av datorer. Det senare kallas då för en DDoS (Distributed Denial of Service) eller distribuerad överbelastningsattack. En annan stor del av överbelastningsattacker är de som kräver anslutningar till offrets dator. En SYN-flood är en sådan attack, mer om dessa senare. Andra attacker kan göra så att processorn jobbar för fullt och har lite tid över till det den egentligen ska göra, dom...

\(^{10}\) http://www.pagina.se/itord/default.asp?SokOrd=denial%2Dof%2Dservice

\(^{11}\) http://www.cert.org/tech_tips/denial_of_service.html#1

\(^{12}\) Stuart McClure et al. (2003) Hacking i fokus (s. 611-615)
kan fylla hårddisk- eller minnesplats. Andra attacker hänger eller gör ett system ostarbilt, detta kan ske genom att bara skicka ett felaktigt paket som mottagande system inte kan förstå.

Som man kan se hör punkt ett i CERT:s lista ihop med de två översta i McClure:s. Han har dock delat upp det i de två delarna förbrukning av nätverksresurser samt förbrukning av systemresurser.

Den nästkommande punkten på CERT:s lista är förstörande eller modifiering av konfigureringsinformation. Denna kan jämnställas med sista punkten i McClure:s lista; toutnings- och DNS-angrepp.

Om ett system är dåligt konfigurerat kan angripare lyckas ändra i routers eller DNS-servrar, vilket kan göra ett nätverk oåtkomligt eller oanvändbart.

Fysisk förstörelse finns inte med i McClure:s lista, och innebär alltså att någon fysiskt förstör nätverksutrustning, datorer eller datorkomponenter. Programmeringsfel som McClure nämner är som ovan nämnd attacker mot operativsystem, program eller inbäddade chip som har något programmeringsfel vilket bidrar till att till exempel ett felaktigt uppbyggt paket eller instruktion kan krascha eller göra ett system ostarbilt. Vi kommer i denna uppsats att hålla oss till McClure:s listning av olika typer av överbelastningsattacker.

2.1 Bandbreddsförbrukning


Vad det egentliga handlar om är att angriparen, antingen själv eller med hjälp av så kallade förstärkande element skickar oerhörd mängder paket mot någon av offrets servrar eller nätverksutrustning. Det kan i princip vara vilka sorts paket som helst. Ofta används ICMP ECHO paket, men i alla fäll i teorin kan nästan vilken sorts paket som helst användas.

Det finns en hel uppsjö av olika attackprogram som kan användas för att utföra bandbreddsförbrukningsattacker. Det kan röra sig om enskilda program som en enskild attackerare använder sig av som dock kan använda sig av förstärkande element, det kan vara virus eller maskar som på ett särskilt klockslag eller en viss dag utför en attack. Det finns också mer sofistikerade programvaror som kan skapa och underhålla stora nätverk av så kallade zombies – övertagna datorer som lyder kommandon från en attackerare. De övertagna datorerna har då blivit antingen hackade eller blivit infekterade av någon typ av virus eller trojan, de senare kallas ofta för distribuerade överbelastningsattacker eller DDoS. Här nedan visas ett antal attacktyper och attackeringsverktyg, mycket är taget från McClure, samt från Dave Dittrichs sida om DDoS-attacker.\[13\]

\[13\] http://staff.washington.edu/dittrich/misc/ddos/
2.1.1 ICMP-strömmar

Attackeraren skickar ett stort antal ICMP ECHO REQUEST paket (Ping) mot ett offer. Detta kan göra att mottagaren kan få det svårt att gå igenom alla paket som kommer. Resultatet kan bli att offrets dator blir slöare, hänger sig eller att legitim trafik helt enkelt har svårare att ta sig in och ut.

2.1.2 UDP-strömmar


2.1.3 Smurf


Vid Smurf-attacker kan man räkna på det så kallade förstärkningsförhållandet. Det vill säga hur många gånger fler paket som skickas från nätverket än från attackeraren. Om nätverket skickar 100 paket per mottaget har anfallet alltså förstärkts med 100 gånger.

2.1.4 Fraggle

Fraggle liknar Smurf väldigt mycket, men istället för ICMP paket används UDP. Om ECHO funktionen är lämnad på hos datorerna i ett nätverk kommer de att svara på ett broadcast-anrop, och även om den inte är på så kommer det ändå skickas paket i form av ICMP Unreachable, vilket även det genererar skadlig trafik.

2.1.5 Slammer

Slammer var den mest snabbspredande mask någonsin. Det var antagligen inte utformat att vara ett verktyg för överbelastningsattacker, och heller inte vara något skadedrabbande då masken inte innehöll några farliga element.

till så att IP-nummer slumpades fram och sedan scannades datorn med den adressen. Den stora mängd trafik som genererades av alla maskar som lyckats infektera system gjorde att många routers och switchar gick under samt att tjänster helt eller delvis sluts ut när maskens spridning var som störst.14

2.1.6 Stacheldraht – attackverktyg

Stacheldraht är ett DDoS attack program (stacheldraht är tyska för taggtråd). Programmet är delat i en master del (handler) och en klientdel (agent).


2.1.7 Trinity – attackverktyg


Observera att det finns ett stort antal fler attacktyper samt verktyg.

14 http://www.computer.org/security/v1n4/j4wea.htm
2.2 Utsvältning


2.2.1 SYN-strömmar

SYN-strömmar kan också placeras under bandbreddsförbrukning men brukar oftast klassificeras som en utsvältningsattack. SYN-strömmar är precis som det låter en ström av TCP SYN paket som skickas till ett offer.

Vid vanlig anslutning börjar alltid kommunikationen på detta sätt. Först skickar den dator som vill ansluta ett SYN paket till mottagaren, denna skickar då tillbaka ett SYN ACK paket, och slutligen svarar den ursprungliga avsändaren med ett ACK paket. Detta förfarande brukar kallas ”3-way-handshake”.


2.2.2 E-mailbombning

Om man som företag har en server för e-mail, kan man råka ut för e-mailbombning. Attackeraren skickar helt enkelt tusentals e-mail till ett eller flera konton på servern. Dessutom kan dom vara riktigt stora för att svälta ut systemet ännu mer.

Problem som kan uppstå är att hårddiskplatsen på servern kan ta slut av alla e-mail samt loggar, hastigheten på nätverket kan slöas ned av all trafik som uppstår vid skickandet av e-mailen och hela systemet kan slöas ned när det försöker processa alla inkommande mail.

2.2.3 Stream – attackprogram


Observera att det finns ett stort antal fler utsvältningsattacker att tillgå.
2.3 Programmeringsfel

Med programmeringsfel menas buggar eller säkerhetshål som beror på felaktig eller oaktksam programmering av operativsystem, applikationer samt logiska chip.

Buffer Overflow attacker har alltid varit vanliga, det är en typ av programmeringsfel som attackerare kan använda sig av, men det finns också fler typer. Ibland kan operativsystem eller användarprogram krascha av ett enkelt paket som inte följer RFC-standarder. Även logikchip kan ha programmeringsfel och kan hänga systemet om en felaktig instruktion mottages. Följande lista är ett antal attacker baserade på programmeringsfel.

2.3.1 Teardrop

Teardrop och liknande attacker går ut på att paket ibland måste delas upp i mindre delar - fragmenteras. Denna attack utnyttjar dock detta och sätter uppdelningen lite speciellt. Det första fragmentet ser normalt ut, men det andra fragmentet har en uppdelning som medveten skriver över delar av det första. Denna attack får vissa system att hänga sig eller starta om. Fler liknande attacker är SYNdrop, Boink, Nesta Bonk och NewTear

2.3.2 Ping of Death

Denna attack kan skapa ett buffer overflow läge. Attackeraren skickar ett fragmenterad ICMP Echo Request paket till offret, paketet är dock ihopsatt mycket större än vad som är tillåtet så när offret försöker sätta ihop paketet igen från alla fragment så kan ett buffer overflow skapas och systemet kan hänga sig eller starta om.

Mängder med programmeringsfel kan utnyttjas för att skapa en Dos-situation. Ovanstående lista är bara ett litet smakprov.

2.3.3 Routnings- och DNS-angrepp

En angripe kan manipulera routningstabeller och därmed göra så att legitima användare och nätverk nekas tillträde. Om en attackerare får tillgång till att ändra de viktiga routningstabellerna kan han omdirigera trafiken till ett annat nätverk eller till ett så kallat svart hål, det vill säga ingenstans. I båda fallen skapas en Dos-situation.

DNS-angrepp kan vara minst lika skadliga. Om en angripe har lyckats att ändra adressinformation i en server kan attackeraren skicka användare till ett annat nätverk eller, som ovan skrivet, till ett svart hål. Detta kan också kallas för att förgifta DNS.
2.4 Försvar mot överbelastningsattacker

För att skapa sig ett försvar mot sådana attacker krävs en del riskanalysarbete. Vi har valt att dela upp det i 4 olika kategorier eller processer som bygger på CERT:s tips samt en artikel av Christos Douligeris och Aikaterini Mitrokotsa.

- Förebygga (Intrusion Prevention)
- Skydda (Intrusion Protecting)
- Upptäcka (Intrusion Detection)
- Reagera (Intrusion Reaction)

2.4.1 Förebygga

Bästa sättet att skydda sig mot överbelastningsattacker är givetvis att förhindra att dom startas från första början. Det finns ett antal förslag och metoder för att hindra att attacker nåver sitt mål.

Användning av globalt koordinerade filter

Paket som används i en överbelastningsattack kan spärras innan dom uppgår till en farlig mängd. Nedan följer ett antal exempel på filter som kan användas till detta ändamål:

- Ingress filtrering
  Man kan använda sig av ingress filtrering på sin eller sina routers. Denna filtrering är ett försök att stoppa spoofade – förfalskade paket in till sitt eget nätverk.
  Det går till så att paket kastas om deras källadress inte stämmer överens med sin domäns prefix som är ansluten till routern.

- Egress filtrering
  Man kan säga att egress filtrering är motsatsen till ingress filtreringen. Då ingress filtrerar inåt det egna nätverket så filtrerar egress utåt. Det hjälper inte som skydd mot det egna nätverket men kan hjälpa andra från att bli attackerade.


17 Med spoofning menas förfalskning, ofta talar man om spoofade adresser det vill säga förfalskade adresser
Routningsbaserad distribuerad paket filtrering liknar ingress filtrering men filtrerar ut spoofade paket med hjälp av routningsinformation. En stor nackdel med denna filtrering är att det kräver kunskaper om nätverkstopologier vilket kan leda till skalbarhetsproblem.

Historiebaserad IP filtrering fungerar så att routern filtrerar enligt en förbyggd adressstabell som bygger på anslutningshistorik genom routern. Endast adresser som är använda under en längre tid eller mer frekvent får användas.

### 2.4.2 Skydda


För att skapa listan över prioriterade tjänster måste man även tänka på att vissa tjänster kan kräva att andra också fungerar som de ska. Därför är det bra att veta hur de olika tjänsterna fungerar innan man gör en sådan lista. Exempelvis kräver SNMP (e-mail) att DNS-tjänsten fungerar som den ska.

När man väl gjort en lista över det man ska koncentrera sitt skydd på är det dags att sätta samman en plan över hur man ska sätta samman försvar för sitt nätverk och system.

Dessa punkter bör följas för att skapa ett mer hållbart nätverk:

- Bygga ditt nätverk med överlevnad i åtanke
- Övervaka ditt nätverk för att få fram vad som är ”normalt” för ditt nätverk för att sedan använda den informationen till att se om något inte står rätt till
- Förbereda organisationen runt om nätverket på icke-tekniskt sätt, det vill säga skapa rutiner för folket som jobbar med, och runt nätverket så att det effektivt kan reagera vid ett anfall.
2.4.2.1 Bygg nätverket med överlevnad i åtande

Med överlevnad menas här att nätverket ska kunna erbjuda tjänster, även under attacker samt att vid fel, helt kunna återställas under en inte allt för lång tidsperiod. Målet med att skapa nätverk tåliga mot överbelastningsattacker är att även under en attack kunna erbjuda de viktigaste tjänsterna till sina kunder.

Vi delar upp vårat förfarande i 3 punkter:

1. Separera och sprid ut kritiska tjänster


3. Visa så lite som möjligt utåt om era tjänster och interna nätverkskonfiguration.

2.4.2.1.1 Separera och sprid ut kritiska tjänster


Man kan också dela upp sitt nätverk i olika kollisionsdomäner det vill säga användande av flera hubbar, switchar och VLAN med mera.


Även på enskilda servrar kan man dela upp resurserna, så att man till exempel delar upp filsystemet på operativsystem, användande och loggningsutrymme.

2.4.2.1.2 Ha mer kapacitet än vad som kan tänkas vara brukligt under en normal dag

Vid en dag med hög belastning – legitim som illegitim krävs det mer kapacitet än vad som kan tänkas vara brukligt under en ”normal” dag. Därför måste man vara beredd på att ha resurser för att klara sådana dagar då belastningen rusar iväg. Extra kapacitet kan vara inte bara bandbredd utan även CPU-kraft, minne, TCP-anslutningsbuffrar (som kan hjälpa mot SYN-strömmar) och andra resurser. Man måste ha i åtande att även om man har stor bandbredd så behöver det inte spela någon som helst roll om ens servrar inte hinner med att processa all inkommande trafik.
2.4.2.1.3 Visa så lite som möjligt utåt om era tjänster

För att minska risken för olika anfall bör man visa så lite som möjligt utåt. De viktigaste målen är att för det första utgöra sig att vara ett så litet mål som möjligt för attackerare, det andra man bör göra är att försöka minska skadan som kan ske mot de specifika målen som visas. Dessa åtgärder kan göras att målen uppnås:

1. **Stäng av onödiga tjänster**
   Om inte en tjänst är helt nödvändig för företaget bör den stängas av. Operativsystem är oftaft installerad, efter installation att erbjudas en del tjänster som inte bara kan vara onödiga, utan också vara hot. Ett exempel på det är echo och chargen i *nix-system, om inte dessa är tänkta att användas bör de stängas av då dessa tjänster kan utnyttjas i attacker.

2. **Göm det inre nätverket**
   Att ge ut information om det inre nätverket kan vara farligt, och är dessutom väldigt onödigt. För att undvika att användare utanför nätverket får reda på inre nätverkstopologi och/eller konfiguration kan man använda sig av delad DNS för inre och yttre nätverket, man kan använda sig av Network Adress Translation (NAT) för det inre nätet. ICMP-paket kan blockeras vid nätverkets utkant för att undvika att attackerare kan kartlägga det interna nätet.

3. **Se till att ha systemen uppdaterade**
   Man bör göra rutin av att regelbundet kontrollera att man har de senaste patcharna och säkerhetsuppdateringar, inte bara för applikationer utan även för hårdvaror och operativsystem. Detta kan göra att bland annat maskar får svårare att utnyttja svagheter.

4. **Filtrering**
5. **Lastbalanserade nätverk (Loadbalanced networks)**

Man kan ha lastbalansering på två olika sätt, antingen har man uppdelning i servrar och/eller så kan man ha uppdelning på flera sajter. När man delar upp på flera servrar kan det hjälpa mot utsvältningsattacker, men mot bandbreddsförbrukningsattacker hjälper det föga.

Uppdelning på flera sajter kan hjälpa mot attacker på bandbredden men kan innebära stora kostnader för mindre företag, som inte har lika stor budget att satsa på säkerhetslösningar. Det innebär också tekniska problem såsom överföring och samtidig uppdatering över de flera sajterna.

6. **Honeypots**

Honeypots är när man sätter upp system som kan lura attackerare att anfalla det systemet istället för det riktiga systemet. En annan fördel med att sätta upp en honeypot är att man kan infånga information om nya sorters attacker och verktyg.

7. **Minimera interna servrars beroende av externa tjänster**

Även om man inte själv är utsatt för en överbelastningsattack kan interna servrar råka illa ut om de är beroende av externa tjänster. Om de i sig är attackerade betyder det inte mycket att man själv sitter bakom ett säkert system.

8. **Använd olika operativsystem**


2.4.2.2 **Övervaka ditt nätverk**

För att kunna finna anomalier i ett nätverks trafik, krävs det först att man vet vad som är normalt beteende för det. Saker man bör kolla upp är nätverkets vardagliga prestanda, mätning av användning av olika protokoll och nätverkets trafikflöden.

När man väl lyckats konstatera vad som bör vara normalt kan man lättare notera ovanligare fall som under överbelastningsattack eller under en dag med ovanligt mycket trafik.

Det som bör fokuseras på att övervakas är de resurser som är vanligast som offer för attacker såsom bandbreddsanvändning och routerns CPU - och minnesanvändning. Servrar bör också övervakas. Även här bör man kolla på CPU - och minnesanvändning, men också hårddiskplats och nätverksstatistik som vad olika TCP anslutningar har för tillstånd, om många anslutningar är i fel väntande tillstånd kan man förmoda att servern är under attack. Om möjligt bör denna statistik loggas så att analys kan genomföras vid tillfälle.

Om företagets nätverk är litet, kan det vara möjligt att övervaka varje server och nätverksutrustning, men om det är större kan det vara svårare. Därför bör man i det fallet åter kontrollera sin prioriteringslista över de viktigaste tjänsterna och sätta övervakning på de servrar som tillhandahåller dom. Den viktigaste nätverksutrustningen som backbones, viktigaste routrarna och switcharna och gateway-brandväggar bör också sättas under övervakning.

Det är viktigt att tänka på att övervakningen kan skapa en flaskhals i nätverket, detta kan ske då för häftig loggning i till exempel en router kan göra så mycket av dess beräkningskraft går åt till loggning, vilket kan slöa ned avsevärt vid exempelvis en bandbreddsförbrukningsattack. Vidare så kan trafiken som skapas vid förflyttning av alla loggar till en förvaringsplats, om så sker slöa ned nätverket bakom routern.

2.4.2.3 Förbered organisationen runt om nätverket på icke-tekniskt sätt

Man kan förutom de tekniska delar som vi har gått igenom ovan, även på ett icke-tekniskt sätt minska risken för överbelastningsattacker, samt skador från dessa. Tre steg kan vidtas för att underlätta detta:

1. **Skapa möjligheter för analys**

2. **Skapa en responsplan vid attacker och tilldela resurser till dess underhåll och genomförande**

3. **Skapa en dialog med din/dina ISP :er (Internetleverantörer)**

2.4.2.3.1 Skapa möjligheter för analys

2.4.2.3.2 Skapa en responsplan

CERT/CC har en rekommendationslista över vad responsteam bör veta vid skapande av responsplaner:

- Dokumenterade standardprocedurer om hur man bör återhämta sig och hur man kan undvika liknande händelser i framtiden vid en attack.

- Skapa handlingssätt (policies) för att skydda känslig information, samt vad som bör eller kan delas med andra parter som är inblandade i incidenten som till exempel andra sajter.

- Skapa kontaktlistor som kan användas vid incidenter. Dessa bör innehålla nätverksadministratörer och andra personer som kan vara ansvariga vid en incident. Listan bör innehålla information om vem som ska kontakta och informera vid olika tillfällen och vid olika händelser.

- Definiera vem som har yttersta ansvar att ingripa vid en attack, och vilka som har tillstånd att ingripa utan att först tillfråga en överordnad. Skapa instruktioner för olika göromål som till exempel vem som har rättigheter att prata med pressen om incidenter, och vem som ska arbeta med myndigheter om de ska bli inblandade.

- Bestäm instruktioner för prioriteringsskapande mellan olika incidenter och prioritering av påföljande göromål vid specifika incidenter.

- Bestäm när en incidents tillstånd ska anses vara avslutad, det vill säga när det som bör göras är gjort och arbetet kan anses vara färdigt.

2.4.2.3.3 Skapa en relation till din/dina Internetleverantörer

Vid en överbelastningsattack utförd mot sitt företag, kan det vara smart att tala med sin eller sina Internetleverantörer. Eftersom det är bättre att försöka kväva attacken så långt bort från sitt nätverk så bör man kontakta sin Internetleverantör, då de har kontroll över routers längre från ens företags yttersta gräns.

Ringer man dock för första gången till sin ISP: s kundtjänst första gången man är under attack, kan det ta längre tid än om man redan innan tagit kontakt och kanske bestämt vissa planer och kontaktpersoner med dem. Den informationen kan också läggas till i responsplanen för att snabbt kunna komma i kontakt med viktiga personer vid en attack.

Redan från början när man skriver kontrakt med sin Internetleverantör kan man försöka påverka dom att vara redo för snabb kontakt och hjälp vid attacker. Här följer några punkter man kan försöka få inskrivna i kontraktet:
Fråga om man kan få tillgång till Internetleverantörens prestanda på dess backbone. Om nätet känns slöt, kan man kolla om det är ens eget nätverk som är under attack eller om det är något annat företag som kan vara det som ligger på samma backbone.

Om man betalar sin ISP per skickad eller mottagen byte, kan man försöka få till stånd en lindring av betalning, om man är utsatt för en överbelastningsattack vilken kan få trafiken att skjuta i höjden.

Trafic Shaping kan vara bra om man vid behov kan låta sin ISP sätta på eller stänga av. Det går till så att man kan ställa in tillåten bandbredd för vissa paket och/eller vissa tjänster (Type Of Service eller TOS).

Ibland behöver man inte ta emot vissa sorters protokoll, eller paket till vissa portar. Då kan man låta sin ISP filtrera bort dom så att dom aldrig behöver komma fram till ens nätverk. Detta kan också vara bra att vid behov stänga av vissa protokoll såsom ICMP-paket när man är under attack av en ICMP-ström.

Man kan försöka diskutera fram en maximal responstid som Internetleverantören får ta på sig vid en attack. Detta kan vara viktigt då man snabbt vill återställa sina tjänster när man är under attack.
2.4.3 Upptäcka

Att upptäcka intrång kan hjälpa inte bara att skydda sig mot överbelastningsattacker, det kan också hjälpa andra nätverk och sajter från att bli attackerade. Man kan upptäcka överbelastningsattacker genom att antingen gå igenom databaser med vanliga kännetecken för de olika attackerna, man kan dessutom använda sig av anomalistudier som vi nämnde i punkt 2.4.2.2.

Det finns en del anomalidetekteringssystem som är utvecklade eller under utveckling för att kunna upptäcka överbelastningsattacker. Ett av dem heter NOMAD, det kontrollerar och analyserar statistik i IP-pakets huvud (header) och kan på så sätt finna anomaler i lokala nätverks trafik.

En annan metod att finna dessa anomaler är att kolla på routrars MIB-information. MIB står för Management Information Base och innehåller paket- och routningsdata. Det har visat sig att man kan påvisa vissa överbelastningsattacker vid analys av paketdata från ICMP, UDP och TCP vid kontrollerad trafik, men att det krävs en del vidareutveckling för att systemet ska fungera bra i riktiga nätverksklimat.


För att kunna applicera filter vid en attack, antingen hos ISP: n eller i det egna nätverkets brandväggar måste man naturligtvis veta vilken sorts trafik man måste spärra. Ovanstående verktyg är användbara, likaså användning av IDS-system som exempelvis Snort\(^\text{18}\) eller Netranger\(^\text{19}\). Andra sätt att veta vilken sorts trafik som ingår i en attack är att använda sig av program som kan fånga alla paket under en kort stund. Det kan räcka med att fånga ett visst antal paket för att snabbt kunna fastställa typen av attack man är utsatt för. Om det finns likheter i paketet, såsom speciella särdrag, kan man införa lämpliga filtreringsregler för att snabbt försöka filtrera bort den trafiken.

2.4.4 Reagera

Hur ska man då reagera när man finner sig under attack? Det beror på en hel del variabler såsom företagets nätverksarkitektur, vilken typ av attack det handlar om, om man har analyserat attacktrafiken, möjligheten att filtrera i det egna nätverket, de anställdas kunskaper och handlingsmöjlighet, attackmålets affärsvärde, hur mycket skada som sker inte bara mot målet utan även runt om kring, om företagets ingående anslutning eller anslutningar är mättade av trafiken och hur företagets kunder drabbas.

\(^{18}\) www.snort.org
\(^{19}\) www.cisco.com
Förhoppningsvis ska det, redan innan finns responsplaner för alla eller de flesta scenarier som kan förekomma.

För mindre eller enklare attacker, bör man kunna motstå attacken själv genom att anpassa trafikfiltreringen, spärra adresser från attackerande datorer, anpassa tillåten max bandbredd på inkommande paket av attackerande protokolltyp med mera. Man bör dock tänka på att även om dessa medel används, betyder inte det att den erbjudna tjänsten fungerar som den borde göra då man inte är under attack. Detta eftersom den illa menande trafiken ändå kan ta stor plats i företagets ingående anslutning, samt slöa den paketfiltrerande enheten, om inte den hinner med den stora trafiklasten. Om man anser att attacken som infinner sig är tillräckligt liten att man själv kan undvika den, bör man först följa ovanstående steg för att sedan kontakta sin ISP för att ytterligare minska attackens påfrestningar med hjälp av deras filtreringar längre bort från företagets gränser.

Vid större attacker som helt, eller till väldigt stor del mättar ingående anslutningar bör man genast kontakta sin ISP så att de kan ta itu med attacken, kanske behöver de också hjälp från övriga bandbreddsleverantörer uppströms om attacken är riktigt kraftfull. Därför är det viktigt att hålla goda kontakter med sin Internetleverantör så att de snabbt kan hjälpa till vid sådana lägen. Vid dessa stora attacker hjälper inte alla brandväggar i världen då anslutningen ändå är full med onödig trafik, vilket gör att legitim trafik har mycket svårt att ta sig både in och ut.

När man kontaktar sin ISP måste man ha den information som krävs redo. Exempelvis kan det vara bra för dom att veta när ungefär attacken startade, hur kraftfull den är, vilken typ av paket som används (om det är en eller flera specifika typer) och hur stor skada attacken har.

Oavsett om filtrering sker vid det egna nätverket eller hos en ISP, bör man följa upp om den är lyckades eller om ytterligare filter måste användas. Om man mäter effekten ett filter regelbundet under attacken, kan man komma fram till om attacken ökar eller minskar i styrka eller typ, och därför kan det nära märkliga steg. Om filtrering anses ha lyckats till den grad att tjänsten utan problem kan nås och resultatet är godtaget, bör man ändå fortsätta att mäta effekt samt samlar in data från attacken så att man kan utföra en riktig analys på attacken efter den har avtagit. Vad man har som mål att komma fram till är bland annat attackens typ, källa och trolig anledning, vad attacken gjorde för skada, inte bara på dess mål utan även indirekt, om resursplaner följes och i så fall dess effektivitet och brister, om rimliga resurser blev tilldelade, hur attacken blev detekterad och om man kan förbättra detektionerutiner, värdera kostnaden på skador orsakade av attacken, både förtroende- samt pengamässigt och bedöma rättsliga påföljder.
2.5 Framtida försvar mot överbelastningsattacker


På programfronten kan dels redan befintliga övervakningsprogram samt skyddande program utvecklas ytterligare för användning hos företag, men framförallt kan program framtagna för Internetleverantörer framtas och utvecklas mer. Ett program som automatiskt upptäcker och förhindrar paketstormar borde verka lovande.

Som icke-teknisk lösning som dock egentligen bygger på teknik, borde alla ägare av nätverk lära sig att ett bra skydd också är att skydda andra, och enligt den premissen aktivera filtrering som hindrar spoofade paket att ta sig ut på nätet. Kanske borde denna "netikett" påtvingas av Internetleverantörer eller kanske till och med av myndigheter. Ett annat sätt är att innehavare av nätverk, själva påverkar situationen genom att helt enkel inte godta paket från andra nätverk utan denna filtrering.


Nyare versioner av BGP – Border Gateway Protocol kan hjälpa till med delning av trafiken på ett smartare sätt. Om protokollet kan känna av ledig bandbredd på anslutningar kan det omdirigera trafik på anslutningar med mer ledig bandbredd.

IPSEC kan användas för att skapa autentisering, integritet och konfidens för IP-trafik.

Fler programvaror och protokoll verkar också lovande och kan hjälpa till att motverka överbelastningsattacker.
3. Metod

Vi har valt två snarlika metoder för att genomföra vår insamling utav information till denna uppsats. Dels har vi genomfört en intervju, och den större delen av insamlingen sker genom utskick av frågeformulär till företag.

På både intervjun och frågeformulären har vi valt att göra kvalitativa tester, gentemot kvantitativa, eftersom vi ville få fram mer specifik data än vi skulle ha fått annars.

3.1 Intervju

Ett av vår tillvägagångssätt eller metoder för insamling utav information inom detta ämne var genom intervju. Här valde vi att intervjuas Björn Mattsson, som är systemadministratör på Datorenheten vid Blekinge Tekniska Högskola. Vi valde honom för att vi kände att han kan ge oss information om överbelastningsattacker, mot Blekinge Tekniska Högskola men även mot högskolor runtomkring i landet. Med tanke på hans position på högskolan så besitter han kunskaper om såväl Blekinge Tekniska Högskolas nätverk, som SUNETs nätverk, och kan då, förhoppningsvis, ge oss en mycket god insikt i hur det är dom jobbar med säkerheten där.

Intervjun genomfördes med en förhållandevis hög grad av standardisering, det vill säga att vi själva hade förberett ett frågeformulär som vi läste ifrån under intervju tillfället. Dock kunde det förekomma att vi la till små tilläggssågor under tiden. Om man skall se till graden av strukturering vid intervjun, så var denna av osstrukturerad grad, på så sätt att det inte fanns några fasta svarsalternativ på frågorna, utan han fick maximalt utrymme att svara på frågorna själv.

Vi tog kontakt med Björn Mattsson genom att skicka ett e-post meddelande till honom där vi förklarade vårt ärende och varför vi ville intervjuas honom, varvid vi bestämde att träffas på högskolan för genomförandet av intervjun.

Vid intervjutillfället närvarade vi båda två, samt Björn Mattsson, och intervjun ägde rum i Datorenhetens konferensrum på Blekinge Tekniska Högskola, i etapp VI, på fjerde våningen.

Det fanns ingen tillgång till någon form av bandspelare, så intervjun skrevs ned för hand av oss båda, för att sedan lättare kunna komplettera varandra om eventuella missförstånd eller liknande skulle uppstå vid senare bearbetning.

---

20 SUNET står för "Swedish University Computer Network" och är de svenska högskolornas anslutning till Internet.
21 Runa Patel et. al (1994) Forskningsmetodikens grunder (s. 60-61)
22 Runa Patel et. al (1994) Forskningsmetodikens grunder (s. 60-61)
3.2 Frågeformulär

Det insamlingsätt av ”nya” data, som dock är av störst vikt för oss i undersökningsyften, är de frågeformulär som vi skickat ut till företag runtomkring i Sverige. Dessa frågeformulär är riktade till två olika typer av företag, säljande företag som exempelvis Datorbutiken, samt tjänsteföretag som då kan vara till exempel Lunarstorm som är en webbcommunity för ungdomar, som alltså endast tillhandahåller en tjänst, och inte säljer eller tillhandahåller någon slags produkt.

Vi beslutade oss för att börja med att kontakta företagen ifråga, per telefon, för att på så viss lättare kunna få tag i en person på företaget, förhoppningsvis en systemadministratör eller liknande, som är mera insatt inom just vårt område.

Problemet med de flesta företag är dock att man oftast bara kan få tag i telefonnummer till deras kundtjänst, och de på kundtjänstavdelningen inte alltid vet vart de skall vända sig till, eller ens vem som är systemadministratör på företaget, utan ger då en tipset att maila deras support på exempelvis support@företaget.se och som nog de flesta redan vet, så brukar supportavdelningarna vara väldigt bra på att inte skicka vidare mail till rätt personer, eller så får man inget svar överhuvudtaget.

Frågeformulären vi förberedde var alltså en dokumentfil som vi mailade till företagen ifråga, och frågorna var helt och hållet standardiserade, eftersom hela formuläret förbereddes i förväg, innan vi skickade iväg formulären till företagen. Graden av struktur är dock även här ganska ostrukturerad, eftersom frågorna lämnar utrymme för såväl stora uttömmande svar på tre sidor om man vill det, eller så kan svaret bestå utav tre små ord, vilket är helt upp till den personen som svarar.

Däri har vi samtidigt problemet med utskickade frågeformulär, vilka är väldigt opersonliga till skillnad från en intervju. Vid en personlig intervju är det lättare för den som intervjuar att kunna få ut den typen av svar som man vill ha, exempelvis genom att ställa en följfråga beroende på vad den som man intervjuar har svarat. Risken med våra utskick till företagen är ju faktiskt att om vi har otur, så får vi inte alls så specifika eller uttömmande svar som vi hoppats på, eller så kanske vi inte får något svar alls.

Vi valde ändå den här typen av mailutskick, för att kunna insamla data från lite fler företag än vi haft tid med om vi skulle ha besökt företagen och bett om en personlig intervju med dem. Detta kan vara något att tänka på om man skall skriva en magisterexamen eller liknande, där man har kanske tjugo heltidsveckor på sig, istället för i vårt fall tio.
3.2.1 Tänkbara problem

Som vi redan nämnt här under delen med frågeformulär så kan man stöta på en hel del problem vi denna typen av informationsinsamling. Vi är förmodligen inte de första som har råkat ut för dessa problem, och beklagligt nog, inte de sista heller.

Problemen uppstod redan när vi började ringa runt företag och ville då ha mailadresser till rätt människor, och med rätt människor menar vi i det här fallet systemadministratörer, nätverkstekniker eller annan kunnig personal inom detta område.

Ofta ville kundservice inte ge oss någon mailadress till en specifik person, utan rekommenderade oss, som vi nämnd tidigare, att bara maila deras kundtjänstavdelning så skulle de skicka vidare ärendet till rätt person. Ett annat problem som vi upptäckte när vi skulle maila ut frågeformuläret till personerna ifråga, var att ibland så stämde inte de mailadresser vi fått från företagen. Kan ibland vara en så enkel sak som att en person stavar sitt namn med ”th” istället för ”tt”.

Vad som dock är det som var av mest missnöje för vår del var att av de tio olika företag som vi skickade ut våra frågeformulär till så har inte ett enda av dem svarat på frågorna. Ett par av företagen skickade ett svarssmail på att de hade mottagit vårt mail, men mer än så var det inte.

Vi hade dessutom ett företag som skickade ett svar och bad oss att maila tillbaka ett frågeformulär i en textfil så att dom kunde fylla i deras svar direkt i filen (Vi skickade ut formuläret i Adobe Acrobat’s .pdf-fil för att de är mer operativsystemsoberoende än exempelvis ett Microsoft Office dokument). Fast än vi skickade tillbaka en textfil till företaget som bad oss, så har vi fortfarande inte fått något svar från dem än.

Våra förhoppningar med dessa tänkbara problem är att detta blir läst av andra studenter som också har tänkt skriva en uppsats och vill skicka ut formulär per mail direkt till företag eller även specifika personer på företag.
3.3 Intervjuer – företag

De tänkbara problem som uppstod vid utskicken av frågeformulär till företag gjorde att vi blev tvungna att ändra vårt tillvägagångssätt för att inskaffa den information vi ville ha från företagen.


Eftersom de frågor vi ställde till företagen vi ringt upp byggde på de frågeformulär vi tidigare skickat ut, så kan man då säga att intervjufrågorna vi hade förberett var av en hög grad av standardisering. Vårt upplägg av struktureringen ifråga vid själva intervjuet cittället var ostrukturerad, det vill säga att den lämnade stort rum för den som blev intervjuad att själv svara på frågorna så som han/hon tyckte passade.

Det som ofta gör en intervju bättre än bara frågeformulär är att vid en intervju, eller i alla fall en ostrukturerad intervju som vår, är att man kan lättare få ett mer ingående svar på en fråga man stälte, eftersom man kan ställa följdfrågor, och riskerar då inte på samma sätt att kanske bara få antingen ett Ja eller Nej som enda svaret.

Intervjuerna gick som sagt till på så sätt att vi ringde upp de kontaktpersoner vi hade på företagen ifråga, och bad dem om de ville ställa upp på en intervju över telefon. Vi ställde frågor som intervjuupersonerna sedan svarade på. Dock kunde det förekomma att vi ställde följdfrågor för att ibland kunna få mer utförliga svar, och det hände även att den intervjuade ställte frågor till oss, om det var något som han/hon inte förstod eller kanske hade missuppfattat.

Vad som däremot var väldigt positivt och överraskande för oss, var att alla de personer vi fick kontakt med och bad om en intervju, ställde upp direkt, vilket inte var något vi själva hade räknat med. Samtliga företag som vi intervjuade gick dessutom med på att vi fick använda deras företagsnamn i vårt arbete.

Även vid företagsintervjun uppstod problem, precis som det gjorde vid frågeformulär utskicken. Dessa tar vi upp under tänkbara problem här nedan.

3.3.1 Tänkbara problem

Problemen här var definitivt färre än vid frågeformulärutskicken, där responsen var lika med noll. De problem som uppstod när vi ringde de kontaktpersoner vi hade, var att de oftast var upptagna i möten, eller befann sig inte på sitt kontor och kunde alltså inte svara i telefon. Var ofta att de bara hade en telefonsvarare där vi lämnade meddelande om att vi ville utföra en intervju, men att de sedan inte hörde av sig till oss.
3.4 Litteratur

Vi har använt oss utav litteratur för att finna information om ämnet ifråga och för att få fram kunskap om grundläggande överbelastningsattacker för att kunna få fram en bra beskrivning i vår bakgrund.

Den litteratur vi har använt oss utav är skriven på såväl internationella språk som svenska.
Facklitteraturen ligger till grund som informationskällor genom hela vårt arbete, men till störst del i den teoretiska bakgrunden.

3.5 Internet

Internet idag innehåller enormt mycket bra och användbar information, och att inte utnyttja sig utav den när den finns där vore helt enkelt en förlust av information.
Det man dock skall tänka på vid användandet utav en Internetkälla är att se till så att den är en trovärdig källa, och helst skall andra publikationer på nätet eller i litteraturform, ha refererat till källan ifråga. Större organisationer och myndigheter är även bra referenslitteratur från Internet, som kan räknas som validerade källor. En plats som vi även använt oss utav för att söka information är BTHs biblioteks egen informationssökning databas, ELIN23 som innehåller endast granskade artiklar och publikationer av hög trovärdighetsgrad.

4 Resultat

Resultatet har vi bestämt oss för att dela upp i de olika frågeställningarna som vi valt att besvara i detta arbete. I vår första frågeställning tar vi upp olika sätt för företagen att skydda sig på mot överbelastningsattacker. Efter det så kommer vi att ta upp ifall dagens företag har bra skydd mot överbelastningsattacker eller inte.

Avslutningsvis har vi en sammanfattning av vad vi har kommit fram till i resultatet.

Vårt resultat grundar sig i huvuddel på de genomförda intervjuerna med de fyra företag som vi har fått kontakt med, samt den intervju vi genomförde med Björn Mattsson på Blekinge Tekniska Högskola. Som tidigare nämnt finns dessa intervjuer nedskrivna och är som bilagor till denna uppsats.

4.1 Hur kan företagen skydda sig mot överbelastningsattacker?

Här kommer vi att ta upp en del av de olika sätt vi har stött på för att skydda sig mot överbelastningsattacker.

I den teoretiska bakgrunden tar vi upp grundligt ett par sätt för företagen att skydda sig mot överbelastningsattacker, och här i resultatet kommer vi att diskutera en del av de sätt som kan vara att rekommendera för företagen.

De viktigaste punkterna, tycker vi, i hur företagen skyddar sig mot överbelastningsattacker kommer här nedan, och det är dessa punkter som sedan kommer att redovisas i denna del av resultatet.

- Bra säkerhetspolicy och utarbetad handlingsplan
- Uppdaterat antivirusprogram
- Brandvägg och IDS
- Olika tjänster på olika servrar
- Cacha sina servrar
- System backup
- Utökad kapacitet
- ISP relation
- Defaultinställningar
Bra säkerhetspolicy och utarbetad handlingsplan

Vad vi värderar som det absolut viktigaste, inte bara för det stora företaget, utan även de lite mindre, är att se till att ha en bra utarbetad säkerhetspolicy på företaget, samt att ha en handlingsplan med åtgärder vid en attack. Detta skall inte bara gälla för överbelastningsattacker, utan alla slags attacker som virus, maskar eller kanske till och med vid spam.

Det är hår viktigt att vid utformandet av en handlingsplan, se till att alla berörda personer får vara med och ha en åsikt, så inte en person får jobbet att skriva ihop planen, och sen när den väl behövs är det ingen som kommer att använda sig utav den ändå, för att den inte fungerar att tillämpa praktiskt. Detta för att de personer som handlingsplanen berör, vet oftast själva bäst vad det är de arbetar med, och hur just deras arbete utförs på bästa sätt.

Vad man skall se till att ha med är vem som ansvarar för vad när en attack utförs, så att inte alla sätter sig på var sitt håll och gör samma saker, utan att man har en tillsatt person som ser till att ett visst filter eller en specifik tjänst blir aktiverat.

Uppdaterat antivirusprogram

Eftersom vi ändå nämnde filter, så är det viktigt att se till att man har ett uppdaterat antivirusprogram, och se till att man har färdiga filter för att snabbt kunna stänga av specifika protokoll som exempelvis om man blir utsatta för en UDP-flood, att man då stänger av UDP och endast UDP-protokollet.

Brandvägg och IDS

Som vi nämnt tidigare i denna uppsats så är en brandvägg, i kombination med ett bra IDS något att föredra. Brandväggen för att stoppa de paket som inte skall passera in eller ut ur nätverket och IDS som underlättar vädligt för att på ett tidigt stadien kunna se att man är attackerad, och förhoppningsvis också utav vem eller vilka.

Olika tjänster på olika servrar

Har man möjligheten, så skall man se till att dela upp olika typer av tjänster på olika servrar, så att inte alla tjänster kommer att drabbas av en attack mot en enda server. Har företaget såväl en mailserver och webbserver som en FTP-server, så försök att ha dessa på 3 olika datorer, om möjligheten finns.

Cacha sina servrar

Om företaget har resurserna, så är det en bra idé som många större företag använder sig utav, att man cachar sin websaajt på en annan server än sin huvudserver, så om den blir attackerad, så kan ändå folk komma in på sidan genom en helt annan server. Det händer ofta att företag hyr in sig hos andra företag för att kunna cacha deras webbserver hos dem, vilket kan göra det ännu svårare för attackerare att veta vilka servrar de skall slå ut.
System backup


Att ta backup är viktigt, men viktigt är också att man testar de bakcup:er man gjort emellanåt, så att de verkligen fungerar när de behövs.

Utökad kapacitet

När det kommer till kapacitet, så skall man, om företaget har råd, se till så att man har kapacitet för mer än man vanligtvis behöver, detta för att kunna klara av en mindre överbelastningsattack utan att servern ifråga ska gå ner direkt vid minsta ökning av bandbredden som man inte räknat med.

ISP relation

Något annat att tänka på, är att man ser till att ha en god relation till sin ISP, och att vid en attack, så kan faktiskt de se till att filtrera paket längre bort från ens egna nätverk än vad man själv har möjlighet att göra, vilket i vissa fall kan avvärja en attack mycket lättare än vad man själv hade klarat av.

Defaultinställningar

Vad som låter ganska självklart, men som glöms bort ofta än man tror, är att se till att stänga av de tjänster som inte behövs, eller är i användning, samt att inte köra allting på "default" inställningar, utan att man konfigurerar sin hård- och mjukvara efter företagspersonliga behov.

Även om det kan låta lite klichéartat så handlar det ofta om att bara se till att använda sig utav lite sunt förnuft, och tänka logiskt, men även att man känner till sitt nätverk ordentligt och vet hur det är uppbyggt.
4.2 Har dagens företag bra skydd mot överbelastningsattacker?

Inom denna frågeställning kommer vi att berätta, dels om vilka skydd de företag som vi har intervjuat använder sig utav idag, och sedan kommer vi även att ta upp vad vi har kommit fram till om utifall det är så att företagen har bra skydd eller inte mot överbelastningsattacker. Dessa skydd som vi nämner nedan, är skydd som företag ofta använder sig utav idag och det baseras på de intervjuer vi genomfört med företag, samt intervjun med Björn Mattsson. Samtliga intervjuer finns sist i denna uppsats som bilagor.

Dessa punkter tycker vi är dom viktigaste när det kommer till om företagen har bra skydd mot överbelastningsattacker idag eller inte. Det är dessa punkter som kommer att redovisas i denna del av resultatet.

- Brandväggar
- Blockera specifika IP-nummer
- Hög prioritet på överbelastningsattacker
- Har en klar uppfattning om vad överbelastningsattacker är
- Ingen som jobbar aktivt
- Är inte alltid medvetna om de blivit attackerade eller inte

**Brandväggar**

Ett utav de skydd som de allra flesta företagen som vi har intervjuat, använder sig utav, och litar till mycket stor del på, är just en mycket påkostad brandvägg. Om vi tittar på företaget JME Data AB i Malmö, så använder de sig utav en brandvägg som heter WatchGuard och är bland de ledande märkena inom att utveckla säkra brandväggar. Priset på en sådan här brandvägg kan ligga från allt mellan 20 000-100 000 kronor.

Som sagt, de flesta företagen använder sig av dessa dyrare brandväggar, och hoppas på att detta hjälper dem att bli av med problem som just överbelastningsattackerna.

**Blockera specifika IP-nummer**

Vad företagen oftast gör, vilket även Blekinge Tekniska Högskola gör, för att på ett lätt sätt stoppa överbelastningsattacker, är att man bara ser till att blockera all trafik från den eller de ip-nummer som attackerna kommer ifrån. Vad som dock gör att detta kan bli jobbigt, är vid en distribuerad attack där det handlar om ett hundratal olika datorer som deltar i attacken, och man skall stänga av varenda ett av dem. Annars kan metoden som sagt fungera bra att bara stänga av de anfallande datorernas ip-nummer, tills det att attacken upphör.
Hög prioritet på överbelastningsattacker

Något som var mycket positivt överraskande var när vi ställde frågan till företagen, om utifall att överbelastningsattacker var högt prioriterat eller inte på deras företag. Här svarade tre utav de fyra företagen att det var mycket hög prioritet på överbelastningsattacker, och Anders Johansson på Enjoy menar att går deras webbsajt ner är det ju faktiskt som att stänga igen hela butiken, för det är ju trots allt där hela deras försäljning sker.

Har en klar uppfattning om vad överbelastningsattacker är

Vid samtliga samtal som genomfördes med företagen, hade intervjunpersonerna en bra och klar uppfattning om vad en överbelastningsattack innebär. Intervjunpersonerna hade dessutom väldigt bra definitioner på vad de kopplar ihop med ordet överbelastningsattacker. Det är viktigt att man är uppdaterad och har koll på termen, vilket de också hade. För att man inte uppdaterad på vilka de senaste hoten är, hur ska man då kunna skydda sig mot dem.

Ingen som jobbar aktivt

Av de företag som vi har varit i kontakt med, har vi även upptäckt att där inte finns någon systemadministratör eller liknande som jobbar aktivt med att just skydda företaget från hot, både utifrån och inom deras egna nätverk. Det är viktigt, även om man har väldigt bra brandvägg, att se till att ha någon som jobbar aktivt med säkerheten på företaget. Det kommer nya virus varje dag, nya sätt att komma förbi brandväggar och nya sätt att kunna sabotage nätverken, såväl inifrån som utifrån.

Är inte alltid medvetna om de blivit attackerade eller inte

Vad som var oroväckande bland företagen, var att det ofta förekom att de kunde ha blivit utsatta för överbelastningsattacker vid ett flertal tillfällen, där de inte ens visste om de verkliga blivit utsatta, eller om det bara hade varit något fel med deras servrar. Detta bör ju då betyda att de inte har något ordentligt IDS för att kunna övervaka deras trafik ordentligt. Företaget LunarWorks, som ligger bakom LunarStorm, sade i deras intervju att dom har ett väldigt bra loggningssystem, men det kanske inte alltid räcker, utan man måste även kunna analysera loggarna på rätt sätt, annars tappar loggnngen sin funktion. Här är det även viktigt att se till så att man inte loggar för mycket, för då kommer systemadministratören snabbt att tröttna och orkar inte läsa igenom loggarna ordentligt, vilket kan leda till att viktig information förbigås.

24 IDS står för Intrusion Detection System och är ett program som analyserar trafiken i ett nätverk och försöker även upptäcka och till viss del förhindra intrångsförsök.
Det är ändå när man tänker efter en stund, förståeligt varför företagen prioriterar överbelastningsattacker väldigt högt, även om man jämför med exempelvis spam eller virus. Vi ställde frågan till företagen hur mycket de tror att de kommer att förlora i omsättning samt i kundanseende om deras webbsajt är nere i 24 timmar. På den här frågan kunde vi se att det handlar om stora summor på bara 1 dygn i förlorad omsättning. Företaget Enjoy uppskattar förlusten till mellan 300 000 och 400 000 kronor, och företaget LunarWorks uppger att de tror att man förlorar extremt mycket i kundanseende när deras webbsajt inte är åtkomlig.

Vad som är väldigt enigt för samtliga av företagen som vi har intervjuat, är att de inte vet vad motivet bakom de överbelastningsattacker, de har blivit utsatta för, är. LunarWorks hade en chansning på att folk helt enkelt utför dessa attacker bara för att de vill se om det går eller inte, vilket mycket väl kan vara ett motiv. Vad motivet bakom överbelastningsattacker är, är väldigt svårt att veta, om man inte blivit förvarnad om att attacken kommer att äga rum, vilket börjar bli allt vanligare.

Överbelastningsattacker mot så kallade vadsläggningsföretag är något som blir allt vanligare och vanligare, och här är det ofta så att motivet handlar om utpressning, just för att det handlar om så mycket pengar, så skulle ett sådant företags sida gå ner, kan de förlopa oerhört stora summor på detta.

Motiven bakom attacker mot de företag vi har haft kontakt med, kan vara allt från att man är sur för att en speciell skiva inte finns i lager som man skulle vilja köpa, eller tycker priserna är för höga, eller att man bara vill testa för att se om det verkligen går att utföra.

Som Björn Mattsson på Datorenheten på Blekinge Tekniska Högskola säger, så handlar det väldigt ofta om en ren hämndaktion som är det bakomliggande motivet till många överbelastningsattacker.
4.3 Sammanfattning av resultatet

Här nedan kommer vi att genomföra en sammanfattning på vad det egentligen är vi har kommit fram till i vårt resultat. Har företagen bra skydd som det är? Används de befintliga skydd som finns idag på företagen? Och om inte, vilka skydd finns det egentligen för företagen att tillgå?

Om vi tar oss en ordentlig titt på vad företagen använder för skydd idag, så har dom egentligen inte så bra skydd inte. De har sina brandväggar, som självklart kan hjälpa om de konfigureras på rätt sätt, och har rätt typ av filter. De företag vi har varit i kontakt med har heller ingen person som på något sätt jobbar aktivt med att skydda företagets nätverk, leta upp de senaste virusen, maskarna, överbelastningsattackerna, och försöka se vilka dom senaste skyddskydd dessa är.

Ett, i vissa fall effektivt sätt att skydda sig är som många av dem använder sig utav, är att blockera de datorers ip-nummer som utför attacken, och på så sätt bara vänta på att den skall sluta. Detta är effektivt, men är tidskrävande om det är en väldigt stor attack, men hundratals datorer inblandade.

De resultat vi fick ut från företagen var bland annat, som är väldigt skönt att höra, att företagen faktiskt prioriterar överbelastningsattacker väldigt högt på sin lista. Detta är dock inte helt svårt att förstå med tanke på att företagen förlorar enorma summor pengar ifall deras sajt går ner, om än bara under ett dygn.

Samtliga företag verkar ha en mycket bra uppfattning om vad överbelastningsattacker innebär, vilket är ett viktigt steg i att sedan kunna förstå hur man skall skydda sig mot dem. Vad som däremot inte ser så bra ut, är att många av företagen ibland tror att de har blivit utsatta, men vet inte om det i själva verket är så eller inte. De vet oftast eller i princip aldrig heller vad motivet bakom attackerna är.

Vi har sedan undersökt, och kommit fram till ett par olika sätt för att så bra som möjligt skydda sig mot överbelastningsattacker. Vad vi tycker är väldigt viktigt, och hoppas att de flesta utav företagen har, är att se till så att man har en bra planerad handlingsplan vid en attack, så att alla vet precis vad de skall göra när det väl händer. Eftersom en del av företagen inte riktigt visste ifall de verkliga blivit utsatta eller inte, så rekommenderar vi att man installerar ett bra IDS för övervakning av sitt nätverk, både det interna och det externa.

Något som i och för sig kostar pengar, men är väldigt bra att göra, är att se till så att man kan dela upp de olika tjänsterna man har på olika servrar, så att man inte "lägger alla ägg i samma korg" så att säga. Försöka, om möjligheten finns, att man cachar sin webbserver hos ett annat företag, så att skulle ens egen websaft vara under attack, kan fortfarande kunderna komma åt sidan från en helt annan server.
5. Diskussion

Så, vad kan vi då säga om resultatet i denna uppsats? Vad som har kommit fram ur denna rapport är att företag i Sverige blir utsatta för överbelastningsattacker, och det händer ofta än man kan tro. Det finns skydd att tillgå med, och de används till viss del har vi sett ute på företagen. Dock är attackerna fortfarande ett stort problem, och de kostar företagen oerhörda summor om de blir drabbade.

Något som man tar upp i diskussionen på en uppsats är reflekterande över metodval, vilket vi kommer att diskutera här nedan.

Förutom att lea information inför ämnet i böcker, artiklar, Internet och annan litteratur, så valde vi som en del i arbetet att intervjuar Björn Mattsson på Datorenheten vid Blekinge Tekniska Högskola. Det frågor vi kunde ställa till honom, och den informationen vi fick ut, hade visserligen inte direkt att göra med vilka skydd företagen i Sverige har idag, men vi fick däremot mycket bra information om överbelastningsattacker, hur de praktiskt på BTH går tillväga för att skydda sig mot attacker, och bra erfarenheter från en person som verkligen jobbar aktivt med detta.


Detta blev en bra erfarenhet för oss att tänka på i framtiden, att det är oerhört svårt att få företag att svara på utmailade frågeformulär.


Att vi bara fick intervjuar 4 företag, kan låta lite, jämfört med att vi hade mailat ut till hela 10 olika företag. Men vi anser då att de fyra företag vi fick chansen att ställa frågor till i en intervju istället var "värda" så mycket mer, till stor del för att vi här fick chansen att få mer utförliga svar och kunde även ställa följdfrågor som vi annars inte hade fått chansen att göra om vi bara hade haft våra utskickade frågeformulär.

Något, som vi lärt oss såhär i efterhand, når det gäller insamling av information från företag, så hade det varit bra om vi hade haft tiden, att verkligen besöka ett antal företag, och kunna utföra intervjuer direkt på företaget, och därigenom kunna få fram ett ännu bättre resultat än vad vi fått i denna uppsats. Detta kommer vi att ta upp vidare i våra slutsatser.
Om vi skall ta och ställa det förväntade resultatet, eller med andra ord, vad vi i början av vårt arbete hade satt för mål med den här uppsatsen. Vilka var då våra mål från början?

Jo, vi ville ta reda på vad för slags skydd företagen egentligen hade att tillgå, om några alls, mot överbelastningsattacker.
Har vi fått svar på denna fråga då? Om man ser på vårt resultat så tycker vi att vi har fått bra svar på vilka skydd som är vanligast, om inte för alla företag i Sverige, så i alla fall bland dem som vi har haft kontakt med.

Vad var då det mer för mål som vi satte upp? Vi ville försöka ta reda på vilka slags skydd som det finns för företagen att använda sig utav, och förhoppningsvis kunna ta fram skydd som de idag inte använder sig av. Vad vi fick fram i vår teoretiska bakgrund, var skydd som företagen kan använda sig utav, och inte bara bättre brandväggar, utan allt från att ha en bra säkerhetspolicy, till en bra filtrering för paket eller hjälpprogram för att stoppa just överbelastningsattacker.

Så når det gäller måluppfyllelsen så ser vi detta som ett lyckat erhållet resultat i förhållande till de mål som vi hade utstakade i början av detta arbete.
6. Slutsatser

I slutsatsen tar vi och baserar på det erhållna resultatet vi har fått fram, och gör en bedömning om hur fortsatt arbete kan se ut.

Med tanke på den tid vi har haft på oss, det vill säga tio veckor, eller tjugo halvfartsveckor, så är vi nöjda med det resultat vi har lyckats prestera. Dock så hade vi gärna velat ha längre tid på oss, för att kunna få ett ännu bättre resultat.

Förslag till vidare arbete är att man skulle kunna utföra större intervjuer, blanda in fler företag, och kunna få chansen att besöka företagen och utföra intervjuer på plats. Tror även detta hade gjort att man kunnat skaffa sig en ännu bättre inblick i hur företagens nätverk är uppbyggt och vad det är de behöver skydda bäst, och kanske vad som inte är lika hög prioritet på.

Vad som även skulle vara intressant att se på i framtiden är på de avgränsningar som vi blev tvingade att göra i vårt arbete. Man hade kunnat ta chansen att se skadan av överbelastningsattacker från ISP:s synvinkel, hur det drabbar dem. Något som också hade varit vettigt att titta på är skydd för de personer, vars datorer aktivt medverkar, utan deras vetskap. Alltså de datoranvändare som blir utnyttjade vid dessa attacker, och som brukar ha benämningen ”zombies”.

Alla dessa ovanstående förslag vore intressanta att sätta sig in i och skriva om, kanske att välja ut några utav dem i ett framtida magisterexamenarbete, vem vet…
7. Referenser

7.1 Böcker


7.2 Artiklar


7.3 Internet

NHTCU – National Hi-Tech Crime Unit (UK)
“The Impact on UK business”
Besökt: 2004-04-06

Dave Dittrich - Senior Security Engineer for the University of Washington's Computing & Communications' University Computing Services Security Operations group
http://staff.washington.edu/dittrich/misc/ddos/
Besökt: 2004-05-10

CERT - the CERT® Coordination Center
http://www.cert.org
Besökt 2004-05-10

Snort – IDS system
http://www.snort.org
Besökt 2004-05-11

Cisco Systems
http://www.cisco.com
Besökt 2004-05-11
Computer.org  
http://www.computer.org/security/v1n4/j4wea.htm  
Besökt 2004-05-02

7.4 Källhänvisningar

Här anger vi eventuella böcker som har varit för oss relevanta inom området, men som vi ej har refererat till i uppsatsen.

Appendix I – Intervjufrågor

Intervjun är uppbyggd på öppna frågor utan förbestämda svarsalternativ (läg strukturering). Eftersom intervjun endast riktas mot en intervjuperson används ingen hög grad av standardisering, då ingen jämförelse eller mätning med andra intervjupersoner förekommer.

Bakgrundsinformation: Denial of Service attacker är i ropet. Man kan läsa om företag som blir utpressade av grupper som hotar med att utföra överbelastningsattacker mot företagens servrar om dom inte får en stor summa pengar.

Intervjufrågorna:

1. *Hur skulle Du vilja definiera begreppet överbelastningsattacker?*

   **Svar:** Kommer väl i första hand att tänka på SYN-flood eller UDP-flood vilka är en vanlig form av överbelastningsattacker.

2. *Varför tror Du att överbelastningsattacker är så populärt i dag?*

   **Svar:** Är ett lätt sätt att ”hämnas” på företag eller organisationer som man kanske räkar vara sur på, som har gjort något oförrätt mot någon eller att man tycker att man har blivit felaktigt behandlad med mera. Politiska motiv kan också finnas.

3. *Har BTH dig veterligen blivit utsatt av någon typ av överbelastningsattack? – Vilken typ av attack var det i så fall? (Distribuerad)?*

   **Svar:** Ja det har dom blivit, vid ett antal tillfällen. Vi hade ett så sent som i förra veckan, då en specifik server dator på BTH blev utsatt av en överbelastningsattack. Detta var med allra högsta sannolikhet en hämndaktion då vi hade upptäcktt att det fanns utdelat ”warez” på denna dator, och det stängde vi ner, vilket leddes till att dom som använde servern hämnades med en distribuerad överbelastningsattack med elva deltagande datorer.

4. *På vilket sätt drabbar det BTH att bli utsatt för en sådan här attack?*

   **Svar:** Vad som hände vid det tillfället var att en router i Karlskrona gick ner under en 5-10 minuter på grund av att det var för häftig loggning på den, och under den tiden fungerade inte Karlskronas nät alls.

   Oftast så är det inte särskilt många av BTH:s tjänster som berörs vid överbelastningsattacker och BTH är väldigt skonad mot sådana attacker också. Sunet har dessutom en väldigt bra övertäkt av sitt nät, 24 timmar om dygnet, vilket gör att man oftast kan hantera situationen väldigt snabbt.
5. Vad tror Du syftet bakom en sådan attack mot BTH är?

Svar: Syftet var ju i detta fall att vi hade upptäckt en ”warez” server på en utav våra servrar, och då tog vi ner den helt enkelt, Så responsen på detta blev som oftast, en hämndaktion mot den servern. Andra saker som kan tänkas ligga bakom attacker just mot högskolan kan vara runt antagningarna, att studenter på andra högskolor ”saboterar”, eller någon gammal student som varit missnöjd med utbildningen på skolan. Ett populärt objekt tidigare var Säkerhetslabbets hemsida tidigare, för att folk helt enkelt ville visa att det gick att ta ner den servern också.

6. Vilka övergripande metoder rekommenderar Du för att skydda sig mot dessa attacker?

Svar: Är näst intill omöjligt att ha ett skydd mot DDoS attacker, tack vare att dessa attacker kan ske på så många olika vägar, både TCP och UDP samt även ICMP och finns då inget sätt att skydda sig mot dom. De tidiga överbelastningsattackerna var nästan uteslutande ICMP och då gick det att minska ”rate limit” på den sortens paket. 
Det effektivaste, och det vanligaste sättet att hantera en överbelastningsattack är helt enkelt att strypa bandbredden till den server som blir attackerad, och sedan kolla loggningen bakåt vart det kommer ifrån och strypa servrar bakåt tills man helt enkelt har stoppat attacken så att man kan öppna upp det egna nätet igen. 
Det handlar helt enkelt om att vid en attack, se till att ha kunnig personal på plats, som snabbt kan åtgärda problemen.

7. Har BTH vidtagit några speciella åtgärder för att skydda sig mot överbelastningsattacker?
– Vilken prioritize har överbelastningsattacker jämfört med t.ex. virus, spam etc.

Svar: Som sagt, inga speciella åtgärder har vidtagits för att skydda sig, utan mer för att skydda BTH själva från att deltaga i en överbelastningsattack. Man kan till exempel inte använda BTH: s nät som förstärkare genom att använda så kallad Smurf-attack, när man använder sig av broadcastadresser. BTH kollar också i trafikmönster från enskilda datorer och ”klumpar” av datorer för att undvika att enskilda datorer är med i en överbelastningsattack. Vårt skydd själva är annars som sagt att vi övervakar nätet och loggar trafiken ständig.
Överbelastningsattacker har en hög prioritet av oss, just eftersom om de inte tas om hand så drabbar de ofta en väldigt vital del av BTH. Vi har satt loggnign på viktiga maskiner på BTH just som förebyggande åtgärder vid attacker.
8. **Hur vanligt är det egentligen att högskolor runt omkring i Sverige blir utsatta för överbelastningsattacker?**

**Svar:** Är inte särskilt vanligt, händer lite då och då. Högskolorna har oftast inte så intressanta ”mål” som man vill ät, utan är väl mer i så fall som en liten hämnd, det gick dåligt på en tenta eller liknande. Vad som däremot är vanligare är då att högskolorna själva, ofrivilligt, är med i överbelastningsattacker.

9. **Anser Ni att det är vanligt med överbelastningsattacker mot företag idag?**

**Svar:** Ja, det är det, för företag som ”sticker ut” på något viss, stora företag, säkerhetsföretag eller företag som handlar med kontroversiella produkter som päls och kött. Kan handla om allt från utpressning till bara ren hämndaktion, kanske blivit sparkad och vill ge igen eller bara tycker man fått för lite lön. Har även börjat bli mer och mer mellan företag, konkurrenter och liknande.

10. **Är det något som Ni anser saknas i intervjun, eller frågor som behöver kompletteras med ytterligare information?**

**Svar:** Nej det tycker jag inte. Rekommenderar dock Rune Gustavsson, kanske att ni kan hänvisa till Säkerhetslabbet vid utskick till företag, ser bättre ut än att ett par studenter själva skickar ut frågeformulär.

11. **Vet Du vart vi kan hitta mer information om detta ämne, kanske några bra tips på böcker, artiklar eller Internetsidor med bra information om just överbelastningsattacker.**

**Svar:** Skulle väl möjligtvis vara [www.grc.com](http://www.grc.com) som är en mycket bra sida. Kanske försöka hitta lite information om IETC också.
Appendix II - Frågeformulär

Frågeformulär (säljande företag)

Överbelastningsattacker är ett aktuellt ämne just nu. Man hör ofta om företag som har blivit utsatta för sådana attacker i olika syften.

Med överbelastningsattacker menar vi alla sorters attacker som gör era nätverksbaserade tjänster otillgängliga, exempelvis en attack mot en webbserver.

Attackerna är paket eller strömmar av paket från en eller flera datorer som, medvetet eller ej, ingår som sändare. Detta kan göra att bandbredden till servern stryps eller att serverns resurser går åt till de anfallande datorerna och inte till de tjänster som egentligen skall hanteras.

Dessa frågor skulle vi vilja att Ni svarar på, gärna så utförligt som möjligt:

1. Vad anser Ni att en överbelastningsattack innebär?

2. Har Ni någonsin råkat ut för överbelastningsattacker? Kunde Ni urskilja vilken/vilka typer av attacker det handlade om? (exempelvis pakettyp, om den var distribuerad eller ej)

3. Om Ni blivit utsatta av överbelastningsattacker, vet Ni vad motivet var bakom dessa attacker mot Er?

4. Vad har Ni för skydd idag mot överbelastningsattacker?

5. Anser Ni att Ni har ett fullgott skydd mot överbelastningsattacker?

6. Har Ni infört några förhindrande åtgärder för att inte själva deltaga i någon form av överbelastningsattack?

7. Tycker Ni att det är hög prioritet på att skydda sig mot överbelastningsattacker? (I jämförelse med exempelvis virus eller spam)

8. Hur mycket anser Ni själva att Ni förlorar i omsättning om era nätverksbaserade tjänster är oåtkomliga under en tidsperiod av 24 timmar? (exempelvis om eran webbsida är nere i 24 timmar)
Frågeformulär (tjänsteföretag)

Överbelastningsattacker är ett aktuellt ämne just nu. Man hör ofta om företag som har blivit utsatta för sådana attacker i olika syften.

Med överbelastningsattacker menar vi alla sorters attacker som gör era nätverksbaserade tjänster otillgängliga, exempelvis en attack mot en webbserver.

Attackerna är paket eller strömmar av paket från en eller flera datorer som, medvetet eller ej, ingår som sändare. Detta kan göra att bandbredden till servern stryps eller att serverns resurser går åt till de anfallande datorerna och inte till de tjänster som egentligen skall hanteras.

Dessa frågor skulle vi vilja att Ni svarar på, gärna så utförligt som möjligt:

1. Vad anser Ni att en överbelastningsattack innebär?

2. Har Ni någonsin råkat ut för överbelastningsattacker? Kunde Ni urskilja vilken/vilka typer av attacker det handlade om? 
   (exempelvis pakettyp, om den var distribuerad eller ej)

3. Om Ni blivit utsatta av överbelastningsattacker, vet Ni vad motivet var bakom dessa attacker mot Er?

4. Vad har Ni för skydd idag mot överbelastningsattacker?

5. Anser Ni att Ni har ett fullgott skydd mot överbelastningsattacker?

6. Har Ni infört några förhindrande åtgärder för att inte själva deltaga i någon form av överbelastningsattack?

7. Tycker Ni att det är hög prioritet på att skydda sig mot överbelastningsattacker?  
   (I jämförelse med exempelvis virus eller spam)

8. Hur mycket anser Ni själva att Ni förlorar i kundanseende om era nätverksbaserade tjänster är oåtkomliga under en tidsperiod av 24 timmar?  
   (exempelvis om eran webbsida är nere i 24 timmar)
Appendix III - Intervjusvar företag

JME Data

Intervjuad person: Mattias Andersson (systemadministratör)
E-mail: mattias@jmedata.se

1. **Svar:** Att det släpps en ny virus-mask på Internet, och då brukar vi mottaga lite varningar i vår webbserverlogg, och våra mailserverloggar.

2. **Svar:** När Blaster-viruset släpptes ut, så gick vår mailserver ner och i princip dog, kom flera 10.000-tals mail på en gång och mailservern blev full direkt. Vår webbshop har inte vad vi vet gått ner av någon attack, utan kan hända ibland att den går ner, men då startar vi bara om den så fungerar den igen. Har ingen avdelning eller grupp som jobbar aktivt med överbelastningsattacker.

3. **Svar:** Nej, det har vi inte, har som sagt vad vi vet inte blivit utsatta för motiverade överbelastningsattacker.

4. **Svar:** Vi har en mycket bra brandvägg som hanterar all trafik mot Internet och bakom den ligger alla våra servrar, butikerna och huvudkontoret. Brandväggen heter WatchGuard ([www.watchguard.com](http://www.watchguard.com)).

5. **Svar:** Det tycker jag faktiskt, med tanke på hur lite vi har märkt av det så tycker jag det.

6. **Svar:** Nej, kan jag inte säga att vi har gjort, förutom vår brandvägg.

7. **Svar:** Vet inte riktigt, vi har nog inte så hög prioritet på det, med tanke på att vi knappt märker av dessa attacker precis.

8. **Svar:** Vi har ungefär 50 % av vår försäljning över nätet, och andra hälften sker i våra butiker, men under en 24 timmars period skulle jag uppskattade det till omkring 200 000 – 300 000kr. Är dock inte så insatt i ekonomi delen av företaget, men skulle gissa på däromkring.

Företagsinformation:

**Namn:** JME Data AB
**Adress:** Pilotgatan 7
212 39 Malmö
**Telefon:** 040-680 31 40
**Email:** info@jmedata.se
**LunarWorks**

**Intervjuad person:** Joacim Åstedt (systemadministratör)  
**E-mail:** joacim.astedt@lunarstorm.se

1. **Svar:** Det är väl när man utsätter de interna interface som finns i en applikation för fullt legitima anrop, fast att det sker i en väldigt extrem omfattning, vilket gör att applikationen inte blir kontaktbar. Kan hända att folk gör script för våra gästboksändringar och skickar iväg 2000 inlägg på en gång eller liknande.

2. **Svar:** Ja, det har vi blivit. Blir med jämna tillfällen utsatta för större eller mindre attacker, oftast sådana som går att stoppa ganska snabbt. Det sker i huvudsak direkt mot Lunarstorm, och inte resten av Lunarworks.

3. **Svar:** Nej det vet vi inte, men misstänker väl att det mest bara är för att se om det går eller inte.

4. **Svar:** Till största delen logiska skydd, dvs. kodmässiga skydd. Vi har även en väldigt omfattande loggning, som ofta gör det möjligt att spåra var attackerna kommer ifrån och på så sätt kunna stänga ute specifika ip-nummer eller rentutav specifika användare också.


6. **Svar:** Ja, det har vi gjort. Vi har begränsad möjlighet till access till våra servrar vilket gör att normalanvändaren bara kan accessa våra servrar på ett sätt, näst intill omöjlig att komma igenom om man inte har rätt behörighet.

7. **Svar:** Ja, det ligger väldigt högt på vår lista. De problem vi har haft är väl ofta när styrelsemedlemmar eller liknande, har pluggat in den bärbara laptopen i vårt interna nät, som de kanske även använder i hemmet. Man måste ha ett bra skydd både utifrån, men nuförtiden även inifrån ens egna nät.

8. **Svar:** Extremt mycket, tror jag.
**Företagsinformation:**

**Namn:** LunarWorks AB  
**Adress:** Södra Hamnvägen 2  
432 22 Varberg  
**Telefon:** 0340 - 641100  
**Email:** info@lunarworks.se
Enjoy

Intervjuad person: Anders Johansson (IT ansvarig)
E-mail: anders.johansson@ellos.se

1. **Svar:** Någon som hackar så att sajten blir överbelastad och inte kan utföra det den skall göra, det vill säga att övriga användare kommer inte åt den.

2. **Svar:** Nej, det har vi inte.

3. **Svar:** -

4. **Svar:** Det vet jag faktiskt inte riktigt, vi outsource:ar hela fronten, dvs. Enjoy's webbsite.

5. **Svar:** -

6. **Svar:** -

7. **Svar:** Ja, det är självlart, definitivt.
   En sajt som utsätts för en överbelastningsattack är ju som att stänga butiken.

8. **Svar:** Skulle gissa på runt 300-400.000kr, förutom självlart att man får "badwill".

**Företagsinformation:**

**Namn:** Enjoy
**Adress:** Box 1718
           501 17 Borås
**Telefon:** 033 – 700 80 00
**Email:** enjoy@enjoy.se
Ginza

Intervjuad person: Gerth Malmevik (IT ansvarig)
E-mail: -

1. **Svar:** Det handlar för oss om 2 allvarliga delar – dels att vårt bredband blir överfullt av skräptrafik, vilket leder till att vi själva inte kommer vare sig ut eller in på vårt nät.

2. **Svar:** Ja, vi har vid ett par tillfällen blivit utsatta. Var förmodligen distribuerade.

3. **Svar:** Har ingen som helst aning om vad för slags motiv som låg bakom.


5. **Svar:** Det har vi väl inte, men som sagt, är inte särskilt ofta som vi blir utsatta för någon typ av attack överhuvudtaget. Sist det hände kunde vi se vilket ip det var ifrån, så då tog vi och blockerade den adressen från vårt nät, så tog attacken slut.

6. **Svar:** Det har vi inte gjort.

7. **Svar:** Vi uppfattar inte oss själva att ligga i riskzonen precis, tack vare att det inte är vi som tillhandahåller webbshoppen, men visst är det hög prioritet på överbelastningsattackar i allmänhet.

8. **Svar:** Svårt att säga, kan inte säga någon siffra på det. Ginza jobbar ju inte bara med webbshoppen utan vi har ju tar också emot order från kataloger, per brev samt med telefon. Så skulle shoppen vara nere har vi alternativ som kan hjälpa oss att ändå få in beställningar.

**Företagsinformation:**

Namn: Ginza Musik AB
Adress: Fåglum
485 81 Nossebro
Telefon: 0512 – 299 50
Email: kundservice@ginza.se

Samtliga av ovanstående företag har gått med på att vi nämner deras namn i vårt arbete.