2002:DS05

EXAMENSARBETE

Personliga brandväggar
Hur säkra är de?

Personal Firewalls
How secure are they?

Stefan Edevåg
Fredrik Hansson

2002-05-22

Högskolan Trollhättan/Uddevalla
Institutionen för informatik och matematik
Box 957, 461 29 Trollhättan
Tel: 0520-47 53 30 Fax: 0520-47 53 99

EXAMENSARBETE

Personliga brandväggar
Hur säkra är de?

Sammanfattning

Allt fler människor kopplar idag upp sig mot Internet med hjälp av höghastighetsanslutningar. Säkerheten har därmed blivit allt viktigare och vi har i den här uppsatsen försökt besvara frågan om personliga brandväggar ger det skydd de utger sig för att göra. Vi har undersökt brandväggarna grundligt, från installation till handhavande, konfigurering och slutligen avinstallation. Vi har med hjälp av olika verktyg tagit reda på hur brandväggen presenterar datorn mot omvärlden. Konfigurering har varit en stor del i arbetet då en väl konfigurerad brandvägg kan fungera utmärkt medan en dåligt konfigurerad brandvägg kan vara en riktigt stor säkerhetsrisk.

Vi har kommit fram till att brandväggarna i sig självt ger ett bra men inte fullgott skydd för privatpersoner. I stort ger samtliga av de testade brandväggarna ett bra skydd under förutsättning att de är rätt konfigurerade, men de behöver användas i kombination med ett väl uppdaterat antivirusprogram för att nå en säkerhetsnivå som får anses som acceptabel. Det är också tydligt att tillverkarna vänder sig till olika typer av användare då vissa brandväggar har betydligt mer omfattande konfigurationsmöjligheter. När det gäller handhavandet är det en smaksak vilken brandvägg man föredrar, men ett par av dem är mer användarvänliga än andra.

Tiny Personal Firewall är den brandvägg vi anser ge det bästa skyddet, men det är under förutsättning att användaren har tillräckligt med kunskap för att konfigurera den förhållandevis avancerade brandväggen. Internet Connection Firewall som medföljer Windows XP tycker vi också är mycket bra alternativ för användare utan några djupare kunskaper i ämnet. De övriga brandväggarna fungerar i stort sett bra och vi vill gärna framhålla att även ZoneAlarm Pro är en bra brandvägg som utmärker sig med bra loggfunktioner och någorlunda bra konfigurationsmöjligheter. Den är dock till skillnad från Tiny inte gratis.

Nyckelord: Personlig brandvägg, säkerhet, konfiguration, skydd

---

Utgivare: Högskolan Trollhättan/Uddevalla, Institutionen för informatik och matematik
Box 957, 461 29 Trollhättan
Tel: 0520-47 53 30 Fax: 0520-47 53 99

Författare: Stefan Edevåg, Fredrik Hansson

Examinator: Stefan Mankefors

Handledare: Christian Olsson

Poäng: 10 **Nivå:** C

Huvudämne: Datavetenskap **Inriktning:** Säkerhet

Språk: Svenska **Nummer:** 2002:DS05 **Datum**: 2002-05-22

DISSERTATION

Personal Firewalls
How secure are they?

Abstract

More people than ever are today connected to the Internet via some sort of broadband connection. Security is becoming more important and we have therefore tested a selection of personal firewalls. We have tested them to see if they protect the computer as well ass they say they do. We have investigated the firewalls thoroughly, from installation and configuration to un-installation. We have used a wide variety of tools to find out how the firewalls present the computer to the rest of the world. Configuration has been very important since a firewall that's not configured the way it should be is a big security risk.

We found that the firewalls do protect the user, but perhaps not as well as they should. It's important that the firewalls are well configured and it's also important to use a updated antivirus software. It is also clear that the manufacturers of the firewalls try to reach different groups of users. When it comes to the administration and configuration, some of the firewalls are a lot user-friendlier.

We think that Tiny Personal Firewall is the best firewall under condition that the user possesses enough knowledge to configure the rather complicated firewall. We also think that Internet Connection Firewall, which is included in Windows XP, is a great alternative for users that doesn't possess the same knowledge. The other firewalls are working well in the test and ZoneAlarm Pro has a great logging functionality. ZoneAlarm PRO is not free though, as Tiny Personal firewall is.

Keywords: Personal firewall, security, configuration, protection

Publisher: University of Trollhättan/Uddevalla, Department of informatics and mathematics
Box 957, S-461 29 Trollhättan, SWEDEN
Phone: + 46 520 47 53 30 Fax: + 46 520 47 53 99

Author: Stefan Edevåg, Fredrik Hansson

Examiner: Stefan Mankefors

Advisor: Christian Olsson

Subject: Computer Science

Language: Swedish **Number**: 2002:DS05 **Date**: May 22, 2002

Innehållsförteckning

1 Introduktion

Internet blir allt populärare i Sverige och fler människor än någonsin kopplade upp sig under mars 2002 (Jupiter MMXI Sverige, 2002). Större delen av befolkningen kopplar fortfarande upp sig med ett traditionellt modem, men andelen personer som ansluter sig via någon form av bredbandsanslutning ökar stadigt. Sverige har under det senaste året fått ett flertal aktörer som erbjuder någon form av bredband (i detta sammanhang kategoriserar vi bredband som en anslutning med minst 512kb/s). I och med att fler datorer kopplas upp mot Internet ökar risken för datorintrång, särskilt i de datorer som har bredbandsuppkoppling. Att bredbandsanslutna datorer utgör en större risk beror på att de oftast är anslutna mot Internet under en längre tid och den högre bandbredden är åtråvärd.

2 Problemområde

Internet har fått en allt större roll i vårt dagliga liv och vi gör bland annat bankärenden, bokar resor, läser tidningen och handlar mat över nätet. I och med att vi blir allt mer beroende av Internet och allt fler kopplar upp sig ökar också hotbilderna. Särskilt utgör bredbandsanslutna datorer en större risk för användaren, då dessa oftast är uppkopplade under en längre tid. Hackare är också oftast mer intresserade av datorer med höghastighetsanslutningar då dessa datorer kan användas vid överbelastningsattacker. Användarna märker inte heller lika lätt om en del av bandbredden går till annat. För att undvika dessa attacker kan en personlig brandvägg användas. Vi avser testa om de vanligaste förekommande personliga brandväggarna ger det skydd som de utger sig göra.

2.1 Frågeställningar

Våra frågeställningar kommer att vara:

- Hur bra skyddar personliga brandväggar mot angrepp utifrån?
- Vilka för- och nackdelar har de olika brandväggarna?
- Hur lätta är brandväggarna att konfigurera på ett tillfredsställande sätt?

2.2 Syfte

Syftet med vår uppsats är att i både teori och praktik undersöka hur säkra personliga brandväggar är. Tyngdpunkten i undersökningen är att undersöka om de personliga brandväggarna verkligen ger de skydd de utger sig göra. Vi kommer även att undersöka hur lätta brandväggarna är att konfigurera. En felaktig konfigurerad brandvägg kan vara en större säkerhetsrisk än att vara helt utan en, eftersom man då tror sig vara säker. En användare utan brandvägg kan vidta andra åtgärder för att skydda sig.

2.3 Avgränsningar

Vår undersökning är avsedd för människor som använder datorn privat. Företag använder som regel inte personliga brandväggar och ingår alltså inte i vår målgrupp. Vi kommer även enbart testa brandväggar som är utvecklade för att köras under Microsoft Windows som operativsystem.

3 Metod

Vi tänker i detta avsnitt beskriva den metod som vi har använt oss av i undersökningen. Vi kommer även att redogöra för hur vi har gjort då vi har samlat in de data som ligger till grund för våra slutsatser.

Inom forskningsmetodiken brukar man skilja på två olika metodiska angreppssätt, nämligen kvalitativa och kvantitativa metoder. Det finns ingen exakt skillnad mellan dessa angreppssätt och det går även att kombinera kvalitativa och kvantitativa element i en och samma undersökning. (Holme & Solvang, 1997)

Vi har valt att använda oss av en kvantitativ metod och undersökningen sker med hjälp av formulär där brandväggarnas egenskaper har delats in i olika kategorier. Vi använder oss av en kvantitativ metod eftersom ett standardiserat upplägg av testerna gör det lättare att jämföra de olika produkterna. Standardiseringen i den kvantitativa metoden gör att alla brandväggar kommer att testas på samma sätt. Då varje brandvägg är indelad i flera kategorier på formuläret kommer varje kategori att betygssättas var för sig. Vi anser att vissa kategorier är viktigare än andra och detta kommer tas i beaktning då vi sammanställer ett slutbetyg för produkten.

3.1 Urval

En population är samtliga enheter av den grupp som vi undersöker. I vanliga fall har man en stor population och det kan då vara tvunget att göra ett urval bland enheterna, eftersom det både är dyrt och tidskrävande att undersöka hela populationen.

Det är viktigt att tänka igenom syftet med undersökningen innan man bestämmer sig för hur urvalet ska gå till. Om syftet är att säga något om populationen så måste man välja ut enheter som är representativa för populationen. (Holme & Solvang, 1997)

Vi har valt att använda oss av ett s.k. ändamålsenligt urval. Detta innebär att man medvetet överger kravet på representativitet. I denna typ av urval är det viktigt att visa att det finns en tanke bakom urvalet och att man kan visa att urvalet är sådant att man får bättre stöd. (Hartman, 1998) Anledningen till att vi inte väljer ett sannolikhetsurval beror på att vi avser endast att testa de mest populära brandväggarna. Eftersom vi utför undersökningen under en tidsbegränsad period hinner vi inte testa alla brandväggar som finns. Vi ville ändå att undersökningen skulle vara relevant för så många som möjligt

och vi valde då att testa de mest populära brandväggarna. Med tanke på detta är det viktigt att tänka på att inte låta resultatet gälla för hela populationen.

Vi har valt att endast testa brandväggar som är utvecklade för Microsoft Windows-plattformen och som finns att tillgå i någon form av shareware/freeware/demo-version. Eftersom vi inte har några ekonomiska medel att röra oss med kan vi tyvärr inte testa de brandväggar som endast finns i betalversioner. De flesta produkter inom detta område kan dock testas gratis i någon form.

Vi har använt oss av Download.com, MajorGEEKS.com, WebAttack.com, ZDNet.com och PCWORLD.com för att ta fram tabeller (se appendix A) över de fem mest nerladdade brandväggarna på varje sida. Vi har därefter valt ut de brandväggar som förekommer på minst två av listorna.

3.2 Formulär

Formuläret (se appendix B) som används i undersökningen är indelat i fem separata avsnitt, nämligen installation, konfigurering, brandväggsfunktioner, avinstallation samt hjälp-funktioner. Formuläret är utformat för att löpande kunna fyllas i under testets gång och frågorna är utvalda och utformade på ett sådant sätt att vi får med det vi anser vara viktigt för en normal användare av en persondator. På en del frågor som kan vara tvetydiga har vi lagt till ett extra kommentarsfält för att kunna belysa de eventuella oklarheter som kan finnas med den aktuella brandväggens funktion. Till exempel är inte fråga A1 (*”Startas brandväggen automatiskt efter installationen?”*) på formuläret korrekt besvarad med ett *’ja’* om man måste starta om datorn för att brandväggen skall fungera. Användaren har då även möjlighet att inte starta om datorn och då startar inte brandväggen automatiskt. Till en del frågor finns följdfrågor som förutsätter ett givet svar i grundfrågan.

Fråga A2 (*”Är det ett intuitivt installationsförfarande?”*) skall ge svar på om installationsförfarandet är intuitivt eller inte. Med intuitivt menar vi att installationen går smidigt och att det inte dyker upp några komplicerade frågor som kan ställa till problem för användaren.

På fråga B4 (*”Kan man ställa in vad som loggas?”*) avser vi alternativ så som om olika händelser kan loggas och om man i så fall kan bestämma ifall händelsen skall loggas eller inte. Vi tar inte ställning till i hur stor utsträckning användaren kan bestämma vad som skall loggas. Det räcker med att det finns någon form av valmöjlighet.

Fråga D1 (*”Raderas alla inställningarna?”*) svarar på frågan om inställningar sparas efter avinstallation. Med den frågan menar vi att en del brandväggar ger en möjlighet att behålla tidigare inställningar efter en ominstallation, vilket kan vara till både fördel och nackdel. En fördel kan ju vara att användaren faktiskt har ett stort antal regler specificerade och att systemet inte ändrats efter ominstallationen och användaren slipper

då skapa dessa regler på nytt. Nackdelen är ju att en ”gammal” regellista kan vara inaktuell och då inte är tillförlitlig ur säkerhetssynpunkt.

När det gäller dokumentationen och fråga E1 (*”Finns manual lätt tillgängligt?”*) har vi inte tagit någon hänsyn till om den medföljer applikationen eller om den finns på tillverkarens hemsida. Det som ligger till grund för bedömningen är om den finns lätt tillgänglig för användaren eller inte. Med lätt tillgänglig menar vi att det finns en tydlig hänvisning till dokumentationen från applikationen.

3.3 Testverktyg

Leaktest:

Leaktest är ett litet program, utvecklat av Steve Gibson på Gibson Research Center (GRC). Leaktest simulerar en trojan och används för att kontrollera om en brandvägg är motståndskraftig mot trojaner. Detta gör det genom att försöka kontakta GRCs server och använda värddatorns port 21 för att skicka en liten mängd data.

Om detta lyckas anser Gibson att det är bevisat att brandväggen är konfigurerad för att tillåta denna trafik eller att den inte klarar av att stoppa den. Webattack.com (2000) är inte helt nöjda med den förklaringen och dom tycker inte att programmet bevisar om en brandvägg är bra eller dålig. Dom väljer att dela in brandväggarna i två grupper, brandväggar som kontrollerar endast inkommande trafik och brandväggar som kontrollerar både inkommande och utgående trafik. Då de konventionella brandväggarna bara kontrollerar inkommande trafik så är det inte speciellt anmärkningsvärt att de inte klarar Leaktest. Dessa brandväggar har som sagt var aldrig utsagt sig kontrollera utgående trafik. Då det gäller den andra gruppen av brandväggar anser Webbattack.com att den enda gången produkterna inte klarar Leaktest är när användaren tillåter programmet att ta kontakt med Internet. Det är då inte brandväggens fel utan fel i konfigurationen från användarens sida. Likväl används programmet i ett flertal av de tester som gjorts av personliga brandväggar och att enbart använda Leaktest som referens för hur bra en brandvägg är, är alltså inte riktigt rättvisande.

Shields UP!:

Även detta test är utvecklat av Steve Gibson och är ett online-test som tar reda på vilken information din dator släpper ifrån sig. Det försöker ta reda på IP-adress, datornamn, och workgroupnamn på datorn. Vidare försöker den koppla upp sig mot port 139 och om detta går kontrollerar programmet om det finns några delade resurser (mappar eller skrivare). Det rapporterar också om möjligheten finns att enkelt få reda på MAC-adressen[1]. Som en del av Shields UP! finns även Probe my ports vilket kontrollerar de

[1] En MAC (Media Access Control)-adress är unik och används för att kunna identifiera enheter på ett nätverk. Kan liknas vid ett serienummer.

portar som de vanligaste tjänsterna använder. Testet körs från GRCs server och visar om portarna är öppna, stängda eller t.o.m. gömda.

Sygate Quick Scan:

Sygate erbjuder ett onlinetest som skannar av ett antal av datorns vanligaste portar och försöker detektera dessa portar. Portarna kategoriseras som öppna, stängda eller gömda. I brandväggsloggarna registreras en portskanning från scan.sygate.com. I testet inkluderas även en kontroll (Trojan Horse Scan) över de portar som de vanligaste trojanerna använder.

Securitymetrics portscan:

Securitymetrics är ett företag i säkerhetsbranschen och de erbjuder en fri portskanning online och detta test skannar de portarna där de vanligaste tjänsterna körs eller de portar som har kända säkerhetsbrister. Detta görs för att avgöra om de är synliga eller inte mot omvärlden. Dessutom görs en snabb trojanskanning på de portar där de absolut vanligaste trojanerna verkar.

Blackcode portscan:
Blackcode portscan är ytterligare ett onlineverktyg och det är betydligt mer omfattande än Securitymetrics test. Dessutom presenteras namn på alla portar, eller rättare sagt namnet på den tjänst som normalt körs på porten (se appendix C). Testet är uppdelat i två delar, först en vanlig portskanning och sedan en trojanskanning. Blackcode erbjuder också ett bibliotek där man kan få mer information om de trojaner som eventuellt skulle kunna användas på det skannade systemet eller om man är intresserad, information om de trojaner som dokumenterats genom åren.

3.4 Metodgranskning

Eftersom vi ska utföra en undersökning som bygger på mätning av olika egenskaper hos ett objekt är validitet och reliabilitet mycket viktigt.

Med validitet menas att man enbart mäter det som avses att mäta (Wallén, 1993). För att få en hög validitet utgick vi från vår frågeställning när vi bestämde oss för hur vi skulle testa brandväggarna samt vilka verktyg vi skulle använda oss av.

4 Teoridel

Andelen Internetanslutna datorer i världen växer för varje dag, så även i Sverige. En dator som är ansluten till någon form av nätverk utsätts alltid för en säkerhetsrisk och givetvis är det inget undantag när det gäller världens största nätverk, Internet. En stor del av de datorer som kopplas upp är datorer som ägs av privatpersoner och även om denna grupp ofta inte är det primära målet för hackare så finns det ändå en risk för att utsättas för obehöriga intrång. Dessa datorer kan användas av hackare till allt möjligt, från att lagra material på dem till att utnyttja flera datorer till överbelastningsattacker

mot andra datorer eller system. Då det finns ett flertal olika hot ska vi specificera de vanligaste.

Trojaner är ett av de större hoten. Precis som namnet antyder är det ett program som utger sig ha en viss funktion men som även innehåller andra, skadliga funktioner. Trojanerna används ofta för att ta över och fjärrstyra datorer. Datorerna kan sedan samordnas till större attacker (se DDoS nedan). Trojaner kan även användas för att hämta information från det infekterade systemet, såsom lösenord och kreditkortsnummer.

Spyware är produkter som använder Internetuppkopplingen i bakgrunden utan att användaren vet om det. Produkten samlar information om användaren och hur denne beter sig och skickar sedan dessa data till tillverkaren. Ofta innehåller reklam-finansierade produkter spyware.

DoS är en förkortning av Denial Of Service vilket innebär att dator A sänder så mycket information till dator B att den blir överbelastad vilket i sin tur leder till att en tredje dator inte får tillgång till tjänsterna på den attackerade datorn (dator B). Dator B kan alltså inte erbjuda de tjänster som övriga datorer efterfrågar vilket i ett företags ögon leder till inkomstbortfall och/eller badwill.

DDoS är en förkortning av Distributed Denial of Service och betyder att ett flertal datorer attackerar ett och samma mål (*se bild 4.1*). Meningen med detta är att skicka så

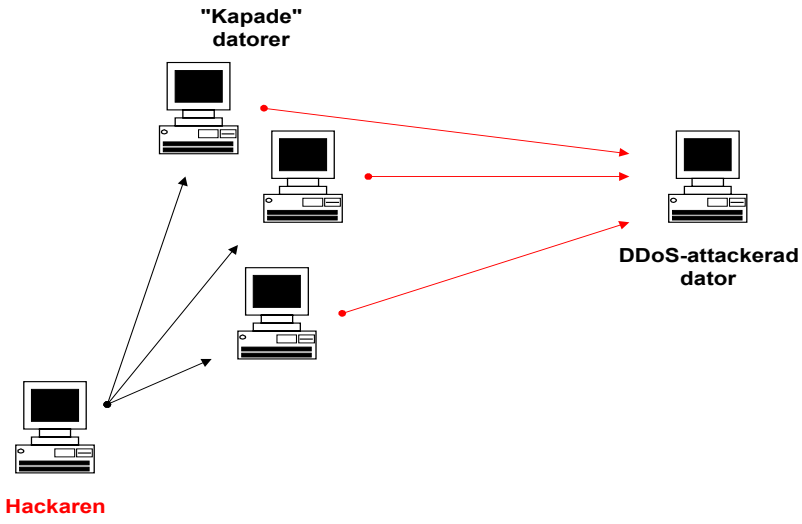

Fig 4.1- En hackare tar över ett par datorer som sedan samordnas för en överbelastningsattack mot en annan dator.

mycket trafik att den utsatta datorn/systemet inte klarar av att ta emot all data. På detta sätt kan man ta ner systemet. Oftast utförs detta med hjälp av ”kapade” datorer och en person kan använda sig av hundratals datorer utan att ägarna till de ”kapade” datorerna märker något. Ur brandväggssynpunkt är det viktigt att tänka på att brandväggen inte skyddar mot attacken i sig utan att det skydd brandväggen kan ge är att förhindra att datorer blir ”kapade”.

En **exploit** drar nytta av svagheter i ett system för att kunna hacka systemet. När väl en hackare har upptäckt en exploit kan s.k. script-kiddies[2] använda sig av den också.

4.1 Vad är en brandvägg?

Nationalencyklopedin definierar en brandvägg på följande sätt:

> *”brandvägg (eng. firewall), i datasammanhang en säkerhetsmekanism som förhindrar oönskad tillgång till delar av Internet. Ett företag kan sätta upp en brandvägg som gör dess interna information omöjlig att nå utifrån. Brandväggen släpper igenom trafik endast till i förväg tillåtna IP-nummer. Den kan också vara knuten till en viss tjänst, t.ex. filöverföring.”*

Brandväggen är till för att trafik från Internet eller något annat publikt nätverk skall kunna kontrolleras. Likaså är det så att information från det privata nätet skall kunna kontrolleras för att inte icke-auktoriserade applikationer skall kunna ta sig utanför det privata nätet (exempelvis trojaner). Brandväggen jämför nätverks- och transport-protokoll med regler lagrade i en databas och släpper bara igenom de paket som i databasen specificerats som godkända.

Följande komponenter ingår i en brandvägg (Perkins, Strebe, 2000):

- Paketfiltrering

Filtrerar bort anslutningsförsök från inte godkända datorer samt till inte godkända tjänster.

- Network Address Translation (NAT)

Översätter (maskerar) interna IP-adresser för att de inte skall synas utanför brandväggen. NAT är i grunden en proxy och funktionen innebär att en enda värddator gör förfrågningar för alla datorer på nätet. På detta sätt döljer man övriga datorers IP-adresser.

- Proxytjänster

Gör anslutningar på uppdrag av interna värddatorer. Med en proxy på programnivå kan trafik av protokoll på nätverksnivå helt förbjudas och istället tillåts bara trafik på högre nivåer (HTTP, SMTP eller FTP).

En brandvägg tillhandahåller i de flesta fall även följande tjänster (Perkins, Strebe, 2000):

- Krypterad autenticering

[2] Personer utan egentliga kunskaper som bara utnyttjar verktyg eller svagheter som upptäckts av andra.

Användare på det publika nätet skall kunna logga in på det privata nätet. Detta skapar vissa problem då brandväggen måste ligga och lyssna på anslutningsförsök på en port och då faktiskt talar om för hackare att den finns.

- Krypterade tunnlar eller VPN (Virtual Private Networking)

För att kunna upprätta en säker anslutning mellan två geografiskt skilda privata nät över internet.

Då vår ambition är att utvärdera ett urval av befintliga brandväggar för personligt bruk och inte beskriva arkitekturer eller design av brandväggar så rekommenderar vi boken Brandväggar 24sju, Pagina Förlag, 2000 som ger en mycket bra översiktlig bild av brandväggar, dess komponenter och arkitekturer.

4.2 ICSA Certified Personal Firewalls

TruSecure Corporation, som är en världsledande organisation inom säkerhet jobbar för att hjälpa företag att identifiera, åtgärda och minska risken för läckage av information. Basen för detta arbete utgörs av ICSA (International Computer Security Association) labs som i över ett decennium jobbat med att certifiera brandväggar, antivirus-program och krypton. ICSA anordnar också konsortium för att ledande krafter inom säkerhetsindustrin skall kunna ha ett forum för utbytande av information.

TruSecure ger också månadsvis ut Information Security Magazine som är den ledande publikationen inom säkerhetsindustrin. Det är också TruSecure som publicerar NT bugtraq[3] som är ett väl använt online-forum för personer i säkerhetsbranschen.

4.3 PC Firewalls

PC Firewalls (eller personliga brandväggar) är enligt TruSecure ”software programs designed to protect an individual host (workstation or laptop) computer while connected to the Internet”, dvs programvara för att skydda individuella datorer uppkopplade mot internet.

Enligt ICSA skall en certifierad brandvägg ha följande grundläggande egenskaper:

- Den skall kunna installeras av en icke-expert.
- Det skall finnas möjlighet att stödja MS Networking utan att säkerheten förbises.
- Det skall finnas möjlighet att stödja samtidiga modem- och LAN-uppkopplingar.
- Den skall ge ett konsekvent skydd trots flera successiva modemuppkopplingar.
- Den skall kunna blockera externa nätverksattacker.
- Den skall kunna begränsa utgående nätverkskommunikation.

[3] http://www.ntbugtraq.com

- Den skall kunna logga händelser på ett konsekvent och meningsfullt sätt.

Målet för ICSA är att certifiera kommersiella produkter för att sätta en stämpel av tillförlitlighet och säkerhet på dom. Enligt ICSA skall en kandiderande brandvägg uppfylla de kriterier som redovisas i appendix D.

Dessa fyra produkter har till och med den 3 maj 2002 blivit tilldelade ICSA PC FIREWALLS CERTIFICATION:

- Sygate Personal Firewall Pro, Sygate Technologies, Inc.
- Norton Personal Firewall 2002, Symantec Corporation
- Tiny Personal Firewall, Tiny Software
- ZoneAlarm Pro, Zone Labs

4.4 Testade brandväggar

Här följer en beskrivning över de brandväggar vi ska testa.

4.4.1 Tiny Personal Firewall

Systemkrav:

CPU	80586 eller högre
RAM	16 MB
Hårddiskutrymme	1 MB
Operativsystem	Windows 9x/Me/NT/XP

Tiny Personal Firewall kräver återstart efter installation.

Tiny Personal Firewall är indelad i tre olika delar vilka alla kan startas var för sig från startmenyn:

- Brandväggen
- Administrationsverktyget
- Status visare *(Status monitor)*

Brandväggen:

Brandväggen måste vara igång innan man kan få tillgång till administrationsverktyget.

Administrationsverktyget:

Administrationsverktyget är det verktyg du använder när du vill konfigurera din brandvägg.

Statusvisare:

Statusmonitor är verktyget för att se vilka applikationer som är bundna till vilka portar.

Information som presenteras i statusvisaren:

Applikation (Application)	Namnet på den applikation som har en tillåten öppen förbindelse
Protokoll (Protocol)	Specificerar om applikationen eller servicen är bunden till TCP eller UDP.
Lokal adress (Local address)	Din dators adress + porten som applikationen eller servicen är bunden till.
Mottagaradress (Remote address)	Adress + port på den dator varifrån informationen hämtas.
Tillstånd (State)	Lyssnar (Listening) i normalfall, förbindelse bruten (connection out) om ingen förbindelse är etablerad.
Etableringstid (Creation time)	Anger tidpunkt för senaste etablerade förbindelsen.
Rx	Mottagen data.
Tx	Skickad data.

För att Tiny Personal Firewall skall fungera på bästa sätt bör den köras som en service. Detta är enda sättet som till 100% säkerhetsställer att brandväggen fungerar direkt efter det att kommunikation till och från datorn är möjlig. Detta gör att de uppsatta reglerna följs innan till exempel en trojan kan ta emot eller sända data.

Tiny Personal Firewall erbjuder tre olika säkerhetsnivåer:

Don't bother me	Den mesta och vanligaste trafiken tillåts.
Ask me first	Standardinställningen. Blockerar all nätverkstrafik och tvingar användaren att sätta upp regler för denna. Det finns en uppsättning fördefinierade filtreringsregler och funktionen "*ask for action when no rule is found*" bör vara påslagen för att med hjälp av en wizard enkelt kunna skapa egna nya filtreringregler. Om inte funktionen är påslagen kastar brandväggen alla paket som inte finns definierade i databasen. Det finns också en funktion för att begränsa inkommande/utgående paket från en speciell IP-adress.
Cut me off	All trafik blockeras.

Loggar:

Det finns en funktion för att separat logga alla händelser som matchar mot en speciell regel. Det går även att skicka alla loggar till en speciell syslog-server.

4.4.2 ZoneAlarm 2.6

Systemkrav:

CPU	80386 eller högre
RAM	8 MB
Hårddiskutrymme	3 MB
Operativsystem	Windows 9x/Me/NT/2000/XP

ZoneAlarm kräver ingen återstart efter installation och erbjuder tre olika säkerhetsnivåer för Internet och lokalt nätverk. Man kan ha olika säkerhetsnivåer på Internet och det lokala nätverket.

ZoneAlarms gränssnitt består av fem olika paneler:

Fig. 4.2 – Visar gränssnittet hos ZoneAlarm 2.6.

Panelerna

Larm (Alert)	Visar alla larm. Där visas också en summering av den data som skickats/tagits emot under dagen samt inställningar där man kan välja att logga alla larm i en fil eller visa dom som pop-up varje gång de dyker upp.
Lås (Lock)	Här går det att tillåta alternativt blockera all nätverkstrafik. Här finns även inställningar för automatisk låsning, tidsinställd låsning, eller låsning när skärmsläckare går på eller när inte internet används.
Säkerhet (Security)	Här sätts säkerhetsnivåerna och de är förinställda på medium för den lokala zonen samt hög för Internet-zonen.
Program (Program)	Här listas applikationer och vilka regler som gäller. Genom att hålla muspekaren över applikationsnamnet kan man få ytterligare information så som var applikationen är lokaliserad, när de installerades eller namnet på den fil programmet använder för kommunikation över internet.
Konfiguration (Configure)	Här görs inställningar beträffande automatiska uppdateringar och huruvida ZoneAlarm skall köras vid uppstart osv. Här finns också registreringsinformation.

Gränssnittet erbjuder också information om upp- och nedladdning av data, vilka applikationer som använder Internet, en hjälpfunktion samt en stoppknapp som omedelbart stoppar all nätverkstrafik.

Loggar:

ZoneAlarm loggar alla larm i filen ZAlog.txt. Larm uppkommer vid följande tre händelser:

FWIN	Indikerar att en inkommande förfrågan om anslutning till datorn blockerats.
FWOUT	Indikerar att en utgående förfrågan blockerats.
PE	Indikerar att en applikation på datorn vill ansluta till internet.

4.4.3 ZoneAlarm Pro

Pro-versionen är precis samma brandvägg som ZoneAlarm, men med några tillägg:

- Den detekterar e-post med bifogade filer och om filtypen är någon av de mer än 40 fördefinierade filtyper som finns i brandväggen, så sätts den i karantän. Detta gör att du får en fråga om du verkligen vill exekvera filen om du t.ex. har fått en exekverbar fil tillsänt dig via e-post.
- Den erbjuder dessutom lösenordsskydd av konfigurationen, fler och mer avancerade konfigurationsmöjligheter samt möjligheten att konfigurera ett ICS[4] nätverk.
- Loggningen är mer avancerad och det finns en funktion för att arkivera loggarna.
- ZoneAlarm Pro detekterar automatiskt nya nätverk och man får välja om nätverket skall klassas som den lokala zonen eller som Internet-zonen. Den låter dig ytterligare konfigurera Internetzonen och den lokala zonen genom att låta användaren tillåta eller blockera olika portar.
- ZoneAlarm Pro har dessutom ett annat gränssnitt (*se fig 4.3*). Gränssnittet påminner mycket om ett webbgränssnitt.

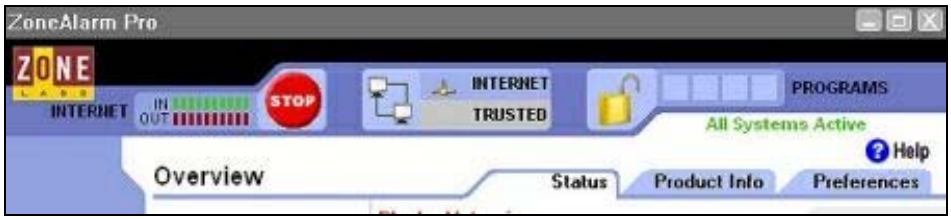

Fig 4.3 – Visar gränssnittet hos ZoneAlarm PRO

[4] ICS – Internet Connection Sharing. Innebär att om en dator i ett lokalt nätverk är uppkopplad mot Internet så kan internetuppkopplingen delas ut till de andra datorerna i nätet. Den datorn som är uppkopplad mot nätet fungerar då som router.

4.4.4 Sygate Personal Firewall

Systemkrav:

CPU	80586 eller högre
RAM	32 MB
Hårddiskutrymme	10 MB
Operativsystem	Windows 9x/Me/NT/2000/XP

Sygate Personal Firewall kräver återstart efter installation.

Sygate erbjuder tre olika nivåer av säkerhet:

- Blockera allt *(Block all)*
- Normal *(Normal)*
- Tillåt allt *(Allow all)*

Under menyalternativet verktyg *(tools)* finns möjligheter att göra inställningar beträffande regler, läsa loggar, eller bestämma huruvida brandväggen skall köras vid uppstart eller inte. Brandväggen erbjuder även lösenordsskydd av konfigurationen.

Gränssnittet består av grafer som visar trafikflödet (*se figur 4.4*) och en kryssruta för att välja om man vill visa Windows services eller inte. Vidare visas ett fönster med exekverande applikationer. Ett meddelandefönster, verktygsfält och menyer underlättar handhavandet för användaren.

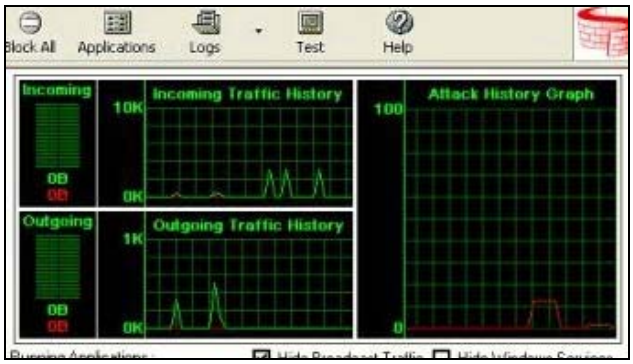

Fig. 4.4 – Graferna visar trafikflödet.

Fyra separata funktioner loggar de händelser som inträffar:

Operationella händelser *(Firewall operation)*	Här loggas de vardagliga händelserna. Loggarna markeras med tre olika ikoner som symboliserar fel, varning eller information vilket gör det lätt för användaren att se om något gått fel eller om systemet bara vill informera om en händelse.
Attackförsök *(Attempted attacks)*	Här loggas intrångsförsök och loggarna markeras med tre olika ikoner som symboliserar kritiska *(critical)*, betydelsefulla *(major)* eller obetydliga *(minor)* beroende på hur allvarliga försöken anses vara
Nätverkstrafik *(Network traffic)*	Här loggas nätverkstrafiken. Loggarna markeras med sex olika ikoner som symboliserar inkommande tillåtna/blockerade, utgående tillåtna/blockerade, riktning okänd tillåten/blockerad.
Grundpaketdata med detaljer *(raw packet data with details)*	Här loggas paketen med destination och IP-adress. Loggarna markeras med en ikon som symboliserar att ett paket loggats.

4.4.5 BlackICE PC Protection

Systemkrav:

CPU	80586 eller högre
RAM	16 MB
Hårddiskutrymme	10 MB
Operativsystem	Windows 9x/Me/NT/2000/XP

BlackICE PC Protection kräver ingen omstart efter installation.

Installationen är jämförelsevis långsam (*se bild 4.5*), men detta beror på att brandväggen skall skanna hela systemet, skapa checksummor och godkänna installerade applikationer. Distributionen innehåller inget avinstallationsprogram[5]

Bild 4.5 – Installationen av BlackICE tar förhållandevis lång tid, i vårt fall över 10 minuter.

BlackICE erbjuder fyra olika säkerhetsnivåer:

Paranoid (Paranoid)	BlackICE blockerar all ej efterfrågad inkommande trafik. Användbar om man utsätts för upprepade intrångsförsök.
Nervös (Nervous)	Blockerar all ej efterfrågad inkommande trafik förutom interaktiva funktioner på webbsidor så som tex strömmande media.
Försiktig (Cautious)	BlackICE blockerar all ej efterfrågad inkommande trafik som påverkar operativsystemet eller nätverksfunktioner.
Betrodd (Trusting)	Den mesta inkommande trafiken tillåts och alla portar är öppna.

BlackICE har likt många andra brandväggar olika ikoner som symboliserar hur allvarligt intrångsförsöket är. Ikonen i aktivitetsfältet blinkar i den färg som indikerar allvaret i attacken (gul, orange eller röd) Man kan blockera enskilda IP-adresser och portar. Den informerar vid intrångsförsök och noterar datornamn och IP-adress på inkräktaren. Man kan dock inte blockera utgående portar.

BlackICE loggar alla händelser. Man kan välja mellan paketloggning *(packet logging)* eller händelseloggning *(Evidence logging)*.

[5] Ett avinstallationsprogram kan laddas ner separat från tillverkarens hemsida.

Det finns sedan fyra olika sätt att konfigurera paketloggarna:

Loggning påslagen *(Logging enabled)*	BlackICE loggar all nätverkstrafik.
Filprefix *(File prefix)*	Här kan användaren själv sätta namn på loggarna. Väljer man ABC sparas loggarna på formen ABC001, ABC002 osv. Grundinställningen är log, det vill säga att loggarna sparas på formen log001 osv.
Maximal storlek (kbytes) *(Maximum size (kbytes))*	Här kan användaren specificera hur stor loggfilerna maximalt får vara. Grundinställningen är 2048k.
Maximalt antal filer *(Maximum number of files)*	Användaren har här möjlighet att specificera hur många loggfiler som maximalt skall genereras. Grundinställningen är 10.

Händelseloggningen har samma fyra inställningsmöjligheter men betydelsen av dom skiljer sig åt:

Loggning påslagen	BlackICE samlar evidence filer för misstänkta händelser.
Filprefix	Samma som ovan men här går också att lägga på en datumstämpel genom att skriva %d efter prefixet.
Maximal storlek	Samma som ovan.
Maximalt antal filer	Samma som ovan men grundinställningen är 32.

4.4.6 Internet Connection Firewall (Windows XP)

Denna brandvägg ingår i operativsystemet Windows XP och grundinställningen är att brandväggs-funktionen är avslagen och man måste alltså efter installationen själv aktivera brandväggen (*se bild 4.6*).

Bild 4.6 – Konstigt nog är inte den inbyggda brandväggen aktiverad som standard.

Brandväggen ger endast skydd för åtkomst utifrån och brandväggen kan inte aktiveras om datorn är medlem i en domän.

I dialogrutan *Egenskaper* som finns kopplad till varje Internetanslutning kan man göra mer avancerade inställningar, så som att definiera de tjänster som körs på maskinen för att öppna de portar som skall användas. Här går att välja från en fördefinierad lista eller skapa egna definitioner om man till exempel skulle vilja använda sig av andra portnummer.

Under fliken säkerhetsloggning *(Security logging)* kan man genom att bocka i kryssrutor välja om man vill logga droppade paket, lyckade förbindelser eller både och. Där går också att specificera var loggen skall sparas samt dess maxstorlek.

Den tredje och sista fliken ICMP *(Internet Control Message Protocol)* ger användaren möjlighet att definiera vilka felmeddelanden och statusinformation man vill dela med andra datorer i nätverket, eller om man vill svara med tidsstämpel eller inte.

5 Genomförande

Vi valde att genomföra utvärderingen av brandväggarna i ett flertal steg. Det första vi gjorde var att ladda hem de brandväggar som vi avsåg att testa. Därefter installerade vi en brandvägg i taget och dokumenterade händelseförloppet genom att använda det tidigare nämnda formuläret och ta skärmdumpar. Vi tog skärmdumpar på de händelser som vi ansåg vara förklarande för en viss funktion på respektive brandvägg. När en brandvägg väl var installerad testade vi den i fem olika steg. För att få en rättvis bedömning av produkterna använde vi oss enbart av standardinställningarna. Eftersom de flesta personliga brandväggar har ett flertal olika säkerhetsnivåer testades dessa var och en för sig.

Då brandväggen installerats påbörjades själva testet av funktionerna. Vi började testet med att köra programmet LeakTest (*se bild 4.7*), som ofta används av populärvetenskapliga datatidningar vid test av personliga brandväggar. Därefter körde vi ShieldsUP! (*se bild 4.8*) för att få en indikation på vilken information som brandväggen släpper igenom.

Fig 4.7 – Programmet Leaktest har inte lyckats kontakta servern.

Nästa test blev Sygates onlineverktyg för att återigen ta reda på om några portar var öppna eller hur de presenterades för en eventuell attackerare.

Efter detta gick vi vidare med att testa brandväggarna med ett antal onlineverktyg. Både Securitymetrics och Blackcodes tester användes och det kanske kan tyckas att vi i undersökningen gjort fler portskanningar än nödvändigt, men de olika verktygen var olika omfattande och vi ville försäkra oss om att ingen av produkterna var partiska. Till exempel skulle Sygates online-test mycket väl kunna ge ett utslag till Sygates fördel och detta är självklart inte önskvärt.

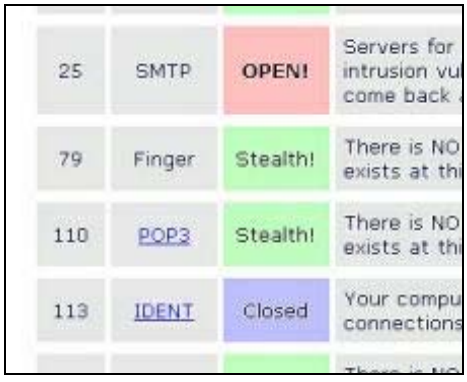

Fig 4.8 – Onlineskanningen ger besked om vilken status de testade portarna har.

Vi gjorde ytterligare ett test på de brandväggar som på något sätt kontrollerar utgående trafik. Detta test gick ut på att se om vi kunde lura brandväggarna att släppa igenom en

icke godkänd applikation. Vi lade till en applikation X i regellistan på de olika brandväggarna och gav på så sätt denna applikation tillgång till Internet. Därefter tog vi en annan applikation (applikation Y) och lade den i samma katalog som applikation X och bytte därefter filnamn på dem. Applikation Y fick alltså det filnamn som applikation X hade när den lades till i regellistan på brandväggen. Vi ville på detta sätt kontrollera att brandväggarna verkligen använder sig av checksummor. Om brandväggen använder sig av checksummor så kommer den nu att neka applikation Y tillgång till Internet.

För att göra det ännu lite svårare för brandväggarna ändrade vi även produkt- och versionsinformationen (alltså den informationen som man får om programmet då man högerklickar på filen, väljer *Egenskaper* och sedan fliken *Version*). För att ändra denna information använde vi oss av verktyget Resource Hacker[6].

6 Testresultat

Installationsförfarandet var mycket lika mellan de olika brandväggarna. Det var intuitivt och efter installationen startade alla brandväggar automatiskt på något sätt, antingen genom att datorn startades om eller att man svarade ja på frågan om brandväggen skulle startas. Den enda brandväggen som aktivt måste startas var Internet Connection Firewall. När det gäller konfigurationen märktes det tydligt att tillverkarna fokuserat på olika områden. Det finns två grupper av brandväggar, de som bara kontrollerar inkommande trafik och de som dessutom har mer avancerade funktioner för att kontrollera utgående trafik. I den andra gruppen finner vi Tiny Personal Firewall, Sygate Personal Firewall och ZoneAlarm Pro.

En del av de testade brandväggarna ger användaren en möjlighet att ha olika säkerhetsnivåer mot Internet och det lokala nätverket och alla brandväggar utom Internet Connection Firewall har flera fördefinierade säkerhetsnivåer som användaren kan välja mellan. En stopp-funktion finns tillgänglig på bland annat ZoneAlarms och Sygates brandväggar och den fungerar så att den blockerar all nätverkstrafik, det vill säga att effekten blir densamma som om du rycker ut nätverkskabeln. Tiny uppnår samma funktion då användaren sätter säkerhetsnivån till den högsta. Ingen av de testade brandväggarna har någon funktion för att exportera eller importera regellistor.

Alla brandväggar utom Internet Connection Firewall larmar visuellt vid otillåten trafik utifrån eller inifrån. Detta sker ofta genom ett pop-up fönster och ofta kan användaren få mer information om larmet. Denna information varierar mellan de olika brandväggarna, vissa ger mer information och andra ger mindre.

[6] Resource Hacker är ett freeware verktyg som kan användas för att modifiera resurser i 32bitars Windows-program.

Vid avinstallation visade det sig att ZoneAlarm kan installeras igen med dom gamla inställningarna. Detta är dock ett frivilligt val. Slutligen visade sig Tiny Personal Firewall vara den enda brandväggen som inte har någon lättillgänglig dokumentation/manual. Alla testresultat som kommer från formuläret finns i sin helhet i appendix E och resultatet från övriga tester finns i appendix F. När det gäller testet av brandväggarnas kontroll av utgående trafik visade det sig att de brandväggar som kontrollerar utgående trafik klarade testet. De lurades alltså inte av namnbyte eller modifiering av produkt- och versionsinformation.

Leaktest

Det första verktyget som vi använde för att testa de olika brandväggarna var Leaktest. Av alla de testade brandväggarna var det bara Microsofts brandvägg som inte stoppade programmets försök att kontakta Internet. BlackICE registrerar och godkänner alla applikationer som redan installerats på systemet. Detta betyder att vårt test med Leaktest gick till på det sättet att BlackICE installerades först och därefter installerade vi Leaktest. Vi testade även att installera BlackICE på ett system som redan innehöll Leaktest, och vid detta tillfälle släppte brandväggen igenom trafiken.

ShieldsUP!

ShieldsUP! består av två olika delar. Vi började med att köra testet utan brandvägg för att få referensvärden.

Test My Shields

När vi körde testet rapporterade sidan att vår dator hade accepterat en anonym anslutning från en maskin som den inte visste någonting om. ShieldsUP!'s webserver anslöt till vår dators NetBIOS fil- och skrivardelningsport (port 139). NetBIOS används för att dela filer i det interna nätverket. Om man samtidigt är ansluten till Internet med denna port öppen så är det stor risk att man delar ut resurserna till hela världen. Trojaner kan då kopieras till hårddisken. Porten bör vara stängd och utdelade resurser skall vara skyddade med lösenord. Denna port är enligt Gibson det enskilt största säkerhetshålet för en nätverksansluten Windowsmaskin..

Rapporten som genererades innehöll även användarnamnet, datornamnet och vilken arbetsgrupp datorn var konfigurerade att använda sig av. Vidare kunde man även se att datorn hade en utdelad resurs (mappen 'SharedDocs'). Den var dock lösenordsskyddad, men man kunde se att den fanns. MAC-adressen på nätverkskortet kunde också avläsas.

Samma resultat fick vi med ZoneAlarm 2.6 och ZoneAlarm PRO 3 när de var inställda på de lägsta säkerhetsnivåerna. De övriga brandväggarna visade dock inte port 139 och testet kunde inte ens påvisa att den existerade. I vanliga fall rapporterar en port om en uppkoppling mot den accepterats eller om den av någon anledning har nekats. I detta fallet betyder det att brandväggen inte bara har stängt porten utan att den har valt att inte rapportera tillbaka att uppkopplingen har nekats. Porten var alltså gömd för omvärlden.

Probe My Ports

Till att börja med körde vi även detta test utan brandvägg. Fyra av de testade portarna var öppna och resten var stängda. De portar som var öppna var portarna 135, 139, 445 och 5000. Port 135 används av Microsoft för att fjärrstyra services som DHCP server, DNS server och WINS server. Den finns i de flesta Windowssystem och enligt Gibson används den av många osäkra Microsoftservices och skall därför aldrig vara öppen för omvärlden. Den går inte att stänga, så man behöver en brandvägg som blockerar den från extern åtkomst.

Microsoft lade i Windows 2000 till möjligheten att köra SMB (Server Message Block) direkt över TCP/IP via port 445. I andra operativsystem kräver SMB-trafik ett extra lager av NBT (NetBIOS over TCP) för att fungera. Porten finns även i Windows XP och Gibson anser även här att många osäkra services använder denna port och den bör därför stängas för omvärlden. Även här krävs en brandvägg för att göra detta. SMB-protokollet används bl.a. för fildelning. När det gäller port 5000 så används den för Universal Plug'n'Play (UPnP), Microsoft's nya protokoll för att tillåta datorer att automatiskt hitta och kontrollera flera olika tillbehör i det lokala nätverket. Protokollet är påslaget som standard och eftersom det innehåller ett flertal sårbarheter[7] är det viktigt att porten inte kan kommas åt utifrån.

ZoneAlarm 2.6 gav samma resultat som ZoneAlarm PRO 3 på alla säkerhetsnivåer. På den lägsta nivån är ZoneAlarm brandväggarna i stort sett avstängda för inkommande trafik och resultatet identiskt med det som gjordes utan brandvägg. När sedan säkerhetsnivån höjdes ett steg ändrades status på tre av de fyra portarna som var öppna till gömda. Den enda port som fortfarande var öppen i detta test var nu port 5000. De övriga portarna förblev stängda, men inte gömda. När vi sedan ökade till den högsta säkerhetsnivån var plötsligt alla utan port 113 gömda. Port 113 rapporterades fortfarande som stängd.

BlackICE hade till skillnad mot de bägge versionerna av ZoneAlarm bara två portar öppna på den lägsta säkerhetsnivån, nämligen port 135 och 5000. Alla andra portarna rapporterades som stängda. När vi ökade säkerheten och ändrade nivån till *'cautious'* var port 5000 fortfarande öppen, port 113 stängd och resten av portarna gömda. De två sista säkerhetsnivåerna gömde även port 5000, medan port 113 förblev enbart stängd.

Sygate Personal Firewall gav i stort sett samma resultat som BlackICE på den lägsta nivån. Skillnaden var att Sygate gömde port 135, som var öppen i BlackICE. Nästa säkerhetsnivå gav samma resultat som BlackICEs två högsta nivåer. Vi kunde inte testa Sygates högsta säkerhetsnivå då den bröt all nätverkstrafik.

Tiny Personal Firewall döljer alla portar utan portarna 113, 135 och 5000 redan på den lägsta säkerhetsnivån. Port 113 är på denna nivå stängd, medan 135 och 5000 är öppna. Den mellersta nivån gav samma resultat som Sygates mellersta och BlackICEs två

[7] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp

högsta nivåer, dvs. alla portarna var gömda utan port 113 som var stängd. Den högsta nivån på säkerheten gick inte heller här att testa då den bröt all nätverkstrafik.

Till slut testade vi WindowsXPs inbyggda brandvägg, Internet Connection Firewall. Den har bara en säkerhetsnivå och den gav samma resultat som de andra brandväggarnas högsta nivåer. Enbart port 113 syntes som stängd och alla andra var gömda för utomstående.

Sygate Quick Scan

Sygate Quick Scan testar i stort sett samma portar som ’Probe My Ports’ med skillnaden att port 143 saknas och ytterligare sju portar har lagts till testet.

Utan brandvägg fick vi samma resultat som ’Probe My Ports’ och de nya portarna som testas rapporterades som stängda. Även BlackICE gav samma resultat som det första testet på alla säkerhetsnivåer och på den lägsta nivån rapporterades de nya portarna som stängda. Följande nivå gömde fyra av de nya portarna och de övriga tre var stängda. De två högsta nivåerna gömde enligt testet alla nya portar utan port 80 som bara var stängd.

Sygate Personal Firewall rapporterade även den samma värden som på ’Probe My Ports’ och de nya portarna var stängda på den lägsta nivån. Den mellersta nivån lämnade portarna 80 och 113 stängda, medan alla andra gömdes.

Tiny Personal Firewall gav som alla andra samma värden som på ’Probe My Ports’. Av de nya portarna var port 80 stängd på bägge säkerhetsnivåerna och de övriga portarna var gömda.

Internet Connection Firewall rapporterades ha port 80 stängd och övriga portar gömda. Detta stämde överens med resultatet vi fick från ’Probe My Ports’.

Till slut testade vi de bägge versionerna av ZoneAlarm och de gav även här identiska resultat. De nya portarna var stängda på de två lägre nivåerna och på den högsta nivån var det bara port 80 och 113 stängda, de andra var gömda.

Sygate Commonly Used Trojan Scan

Även detta test körde vi utan brandvägg först. Det visade sig då att alla portarna rapporterades som stängda redan utan någon brandvägg installerad på datorn. När vi därefter testade BlackICE så rapporterade även den alla portarna som stängda på de två lägsta säkerhetsnivåerna, men när vi ställde om den till de två översta nivåerna gömdes dock alla testade portar. Sygate gav i stort sett samma resultat som BlackICE då den hade stängt portarna på den lägsta nivån och sedan gömde dem när man gick upp en säkerhetsnivå. Tiny Personal Firewall var den första brandväggen i detta test som dolde alla portar redan på den lägsta nivån och även Microsofts brandvägg dolde alla portarna. ZoneAlarms bägge versioner i testet gav identiska resultat och portarna rapporterades endast som stängda på de två första säkerhetsnivåerna, men de doldes sedan när vi ökade till den översta nivån.

SecurityMetrics

SecurityMetrics test gav resultatet att utan brandvägg var port 139, 445 och 5000 öppna. Övriga portar var stängda. Trojanskanningen visade att alla portar var stängda.

När det gäller BlackICE var istället portarna 139 och 445 gömda på de två lägsta nivåerna och port 5000 var öppen. På de två högsta säkerhetsnivåerna var alla portar gömda. Trojanskanningen visade att de två lägsta nivåerna resulterade i att portarna var stängda och på de två högsta nivåerna var de stängda.

Sygate hade stängt alla portar på lägsta säkerhetsnivån utom port 5000 som var öppen och port 445 som var gömd. Den högre nivån gömde alla portar. Detsamma gällde Trojanskanningen där den lägsta nivån stängde portarna medan den högre gömde dom.

Tiny gömde alla portarna även på lägsta nivån utom port 5000 som var öppen. Port 5000 gömdes på den högre nivån. Trojanskanningen visade att alla portar var gömda.

Internet connection firewall gömde alla portar både för den vanliga portskanningen och för Trojanskanningen.

Zone Alarm gömde alla portar på den högsta nivån medan den på mellannivån öppnade port 5000 medan port 139 och 445 var stängd. På lägsta nivån var alla portar stängda utom port 139, 445 och 5000 som var öppna. När det gäller Trojanskanningen stängde Zone Alarm alla portar förutom på högsta nivån då den gömde portarna istället.

BlackCode Security Scan

Detta verktyg testar en stor mängd portar (se appendix C för komplett förteckning). När vi som vanligt började med att köra testet utan brandvägg visade det sig att portarna 135, 139, 445, 1025 och 5000 var öppna. Fyra av dessa portar hade vi redan i tidigare tester fått rapporterat som öppna, men port 1025 var ny. Denna port är den första dynamiskt tilldelade porten och därför kan i stort sett vilket program som helst som ber om en port tilldelas denna.

BlackICE visade att portarna 135, 1025 och 5000 var öppna på den lägsta nivån, men port 135 stängdes sedan på nivå två. På de två översta nivåerna var alla portarna stängda. Sygate hade även den portarna 1025 och 5000 öppna på den lägsta nivån, men stängde dem när säkerheten höjdes. Tiny Personal Firewall rapporterade samma resultat som BlackICE, dvs portarna 135, 1025 och 5000 var öppna på den lägsta nivån och när säkerheten ökade var alla portar stängda även här. Microsofts Internet Connection Firewall rapporterade alla portar som stängda. ZoneAlarm 2.6 och ZoneAlarm PRO 3.0 hade portarna 135, 139, 445, 1025 och 5000 öppna på den lägsta nivån och resten stängda. På medium nivån var bara port 1025 och 5000 öppna och på den översta nivån var alla portarna stängda.

7 Diskussion

Att jämföra olika brandväggar är inte speciellt enkelt. De är utformade på olika sätt och tillverkarna har valt att lägga tyngdpunkten på olika funktioner. Vissa lägger stor vikt vid användarvänlighet och andra större vikt vid t.ex. konfigurationsmöjligheterna. Det visade sig också att målgruppen för de olika produkterna skiljer sig åt. ZoneLabs vill med ZoneAlarm erbjuda en bra produkt för normalanvändaren som inte behöver ha någon större kontroll över utgående trafik samt inte heller vill göra någon avancerad konfiguration av brandväggen. En annan brandvägg som riktar sig till vanliga hemanvändare är Microsofts Internet Connection Firewall. Den erbjuder inga avancerade konfigurationsmöjligheter mer än att man kan specificera vilka tjänster man kör på den aktuella datorn från en fördefinierad lista. Listan kan även utökas med egendefinierade tjänster. Internet Connection Firewall skiljer sig inte nämnvärt från ZoneAlarm 2.6. Testresultaten över inkommande trafik är identiska när man har ställt in ZoneAlarm på den högsta säkerhetsnivån. Det som skiljer produkterna åt är att det finns en viss möjlighet att kontrollera utgående trafik i ZoneAlarm. Denna kontroll är väldigt enkel och består enbart av att varje gång en applikation vill ha tillgång till nätverket för första gången så måste detta godkännas av användaren. Användaren har inga möjligheter att specificera några regler för hur applikationen får använda nätverket. Detta betyder att när en applikation väl har godkänts att använda nätverket kan den sända och ta emot vilken typ av data som helst, från och till vilken dator som helst. Risken finns också att en ovan användare systematiskt godkänner alla applikationer som ber om Internetåtkomst. ZoneAlarm 2.6 erbjuder heller inte några mer avancerade konfigurationsmöjligheter och vi anser att endast den högsta säkerhetsnivån ger ett acceptabelt skydd.

ZoneAlarm Pro är däremot som en helt annan produkt jämfört med ZoneLabs gratisprodukt ZoneAlarm 2.6. Detta beror antagligen på att denna version inte är gratis och den erbjuder helt andra konfigurationsmöjligheter och den har mycket bra loggfunktioner. En nackdel är dock att det inte går att specificera vilka IP-adresser det skall vara tillåtet att skicka data till eller ifrån vilka IP-adresser man skall tillåta applikationer ta emot data ifrån. Man kan dock specificera vilka portar en applikation får och inte får använda.

Även BlackICE fungerar på samma sätt som ZoneAlarm 2.6 beträffande utgående trafik, men BlackICE ger även möjligheten att öppna specifika portar och den ger också mycket bra information om inkräktaren vid eventuella intrångsförsök. Man kan dock inte specificera vilka nätverk som man vill lita på.

Tiny har visat sig vara en riktigt bra brandvägg, dock är den lite svår att konfigurera för en normalanvändare och det kan också vara lite svårt att få överblick över de uppsatta reglerna. Den består av tre moduler och man kan lägga till nätverk som man litar på. Trafik från dessa nätverk påverkas då inte av brandväggen. När det gäller testerna visar det sig att Tiny i många fall gömmer portarna istället för som många av de andra

brandväggarna enbart stänger portarna. Brandväggen är gratis vilket är en stor fördel , men en stor brist är att det inte finns någon lättillgänglig dokumentation.

Sygates brandvägg är också gratis och har ungefär samma funktioner som Tiny Personal Firewall. På den högsta säkerhetsnivån som fortfarande tillåter nätverkstrafik så är deras testresultat identiska. En viktig funktion saknas dock i Sygates version och det är möjligheten att lägga till nätverk som man litar på.

Slutligen har vi Internet Connection Firewall, brandväggen som är inbyggd i Microsofts operativsystem Windows XP. Denna brandvägg ger ett mycket bra skydd för inkommande trafik. Våra tester visar att den gömmer portar i de flesta fall, istället för att stänga dom, och för att öppna portar för inkommande trafik bockar man bara i de tjänster man vill använda sig av från en fördefinierad lista. Listan över tjänster går att modifiera och man kan även själv lägga till vilka portar man vill öppna. Nackdelar är att det inte finns några större konfigurationsmöjligheter, att den inte kontrollerar utgående trafik och att brandväggen inte är igång då man installerat Windows XP. Men den ingår i operativsystemet och får därmed ses som gratis och ett mycket bra alternativ för den absoluta nybörjaren.

8 Slutsats

Vi anser att Tiny Personal Firewall är den bästa brandväggen för personer med mer än medelmåttliga kunskaper inom datorområdet. För att Tiny skall ge ett bra skydd måste den vara rätt konfigurerad och för en användare med för lite kunskaper kan den verka svåröverblickbar och avancerad (*se bild 8.1*). Men resultaten visar att den i de flesta fall gömmer portarna i stället för att stänga dom och det är en mycket bra egenskap. Dessutom är Tiny Personal Firewall gratis vilket borde vara attraktivt för de flesta hemanvändare. Slutligen skall man heller inte förbise att Tiny Personal Firewall är certifierad av ICSA vilket betyder att den genomgått rigorösa tester både vad som gäller funktioner och användarvänlighet.

ZoneAlarm Pro är ett annat bra alternativ. Den är också certifierad av ICSA och kanske lite lättare att överblicka för en normalanvändare. Dock kostar den pengar och man kan inte heller specificera vilka IP-adresser vissa applikationer skall få ansluta till och ta emot data ifrån.

För den absoluta nybörjaren finns det ingen egentlig anledning att använda någon annan brandvägg än den som följer med Windows XP, förutsatt att du använder det operativsystemet. Testresultaten visar att den gömmer portar istället för att bara stänga dom och trots att det finns ytterst få konfigurationsmöjligheter och en enda säkerhetsnivå så visar den sig klara testerna mycket bra. Den kontrollerar dock inte utgående trafik vilket är en nackdel. Brandväggen arbetar i det dolda och gör ett bra jobb.

Fig. 8.1 – Vissa meddelanden kan verka kryptiska för en normalanvändare.

ZoneAlarm 2.6, Sygate Personal Firewall och BlackICE PC Protection är egentligen inte dåliga, men de hamnar i ett mellanskikt då de inte sticker ut på någon punkt.

ZoneAlarm 2.6 riktar sig till nybörjare och vi anser att man lika gärna kan använda Windows XPs inbyggda brandvägg om man är nybörjare.

Sygates brandvägg riktar sig till samma målgrupp som Tinys, men den saknar möjlighet att specificera nätverk som man litar på.

BlackICE har en riktigt dålig egenskap och det är att den godkänner alla redan installerade program. Om datorn redan är infekterad av en trojan så läggs den till i regellistan och är därmed godkänd att kommunicera via Internet.

När det gäller brandväggar i stort visar det sig ganska snart att de kanske ger användaren en lite falsk säkerhet. Flera av brandväggstillverkarna säger sig stoppa trojaner och det är en sanning med modifikation. Trojaner kan placeras i ett system på flera sätt, bl.a. kan en angripare skicka en infekterad fil till offret via e-post. När användaren kör programmet kan trojanen automatiskt installeras i bakgrunden utan att användaren märker det. Trojanen kommer sedan att vänta på att bli kontaktad utifrån eller så kommer den att försöka skicka data till en förutbestämd adress. Alla brandväggar som vi testade utan Internet Connection Firewall skulle stoppa denna typ av trojan. En trojan kan också se ut på ett annat sett och istället för att installeras när den infekterade filen körs så exekveras trojanen i filen. Den infekterade filen kan t.ex. vara ett oskyldigt online-spel som kräver Internetåtkomst och när användaren tillåter programmet detta har även trojanen full åtkomst till Internet. Delvis går detta att förhindra genom att specificera vilka portar en applikation får använda samt vilken eller vilka IP-adresser den får ta kontakt med.

Ett väl uppdaterat antivirusprogram i kombination med en brandvägg ger ett bra skydd då antivirusprogrammet kan kontrollera virus och trojaner och brandväggen kan

kontrollera att inga icke godkända program ansluter till nätverket. En dåligt konfigurerad brandvägg ger många gånger sämre skydd än ingen brandvägg alls och i sista änden är det användarens sunda förnuft som avgör hur säkert systemet är.

9 Referenslista

Hartman, Jan (1998). *Vetenskapligt tänkande*. Lund: Studentlitteratur.

Holme, Idar Magne & Solvang, Bernt Krohn (1997). *Forskningsmetodik*. Lund: Studentlitteratur.

Perkins, C., Strebe, M. (2000). *Brandväggar 24sju*. Sundbyberg: Pagina Förlags AB

Internetreferenser:

URL 1: TruSecure Corporation (ICSA labs)
http://www.icsalabs.com/index.shtml (2002-04-18)

URL 2: MajorGeeks
http://www.majorgeeks.com (2002-04-18)

URL 3: Download
http://www.download.com (2002-04-18)

URL 4: BlackICE
http://documents.iss.net/manuals/BIPCP_UG_35.pdf (2002-04-18)

URL 5: Sygate
http://www.sygate.com/swat/support/documentation.htm (2002-04-18)

URL 6: Tiny Software
http://www.tinysoftware.com/home/tiny?s=76247047244985866 32A0&la=EN&va=aa&pg=download (2002-04-18)

URL 7: Zonelabs
http://www.zonelabs.com/services/support_za_zap.htm (2002-04-18)

URL 8: Jupiter MMXI Sverige
http://se.jupitermmxi.com/xp/se/home.xml (2002-04-18)

URL 9: ZDNet
http://www.zdnet.com (2002-04-18)

URL 10: PCWORLD
http://www.pcworld.com (2002-04-18)

URL 11: WebAttack
http://www.webattack.com (2002-04-18)

URL 12: Nationalencyklopedin
http://www.nationalencyklopedin.com/jsp/notice_board.jsp?i_type=1 (2002-04-18)

Appendix A - Nedladdningar

15/4-2002

Download.com – nerladdningar senaste veckan

ZoneAlarm 2.6	296,637
Tiny Personal Firewall	22,298
ZoneAlarm PRO 3	16,294
BlackICE	12,920
Sygate 5	5,503

ZDNet.com – nerladdningar senaste veckan

ZoneAlarm 2.6	87,119
BlackICE	3,776
ZoneAlarm PRO 3	2,687
Sygate	2,284
Tiny Personal Firewall	1,491

PCWORLD.com - nerladdningar totalt

ZoneAlarm 2.6	76,216
Tiny	10,469
Sygate	9,304
BlackICE PC	1,371
TermiNet	316

MajorGEEKS.com - nerladdningar totalt

ZoneAlarm PRO	4,838
Kerio 2.1.4	3,618
BlackICE	1,315
Tiny 2.0.15	512
Outpost Firewall Free 1.0.1511	315

WebAttack.com – presenterade inga siffror, bara de populäraste nerladdningarna.

ZoneAlarm	-
Sygate	-
Tiny	-
ZoneAlarm PRO	-
ConSeal PC Firewall	-

Appendix B - Formulär

Namn:

Shareware ☐ Freeware ☐ Annat ☐

A.) INSTALLATION

A1.) Startas brandväggen automatiskt efter installation?

Ja ☐ Nej ☐

A2.) Är det ett intuitivt installationsförfarande?

Ja ☐ Nej ☐

B.) KONFIGURERING

B1a.) Kan man bestämma vilka IP-adresser en viss applikation får ansluta till eller ta emot data från?

Ja ☐ Nej ☐

B1b.) Kan man definiera IP-spann?

Ja ☐ Nej ☐

B2a.) Kan man bestämma vilka portar en viss applikation får använda?

Ja ☐ Nej ☐

B2b.) Kan man definiera portspann?

Ja ☐ Nej ☐

B3.) Kan man öppna specifika portar för trafik utifrån?

Ja ☐ Nej ☐

B4.) Kan man ställa in vad som loggas?

Ja ☐ Nej ☐

B5.) Kan man ställa in var loggen sparas?

Ja ☐ Nej ☐

B6.) Kan man ställa in om loggen skall roteras inom ett viss tidsintervall?

Ja ☐ Nej ☐

B7.) Kan man ställa in en säkerhetsnivå mot det lokala nätverket och en annan mot Internet?

Ja ☐ Nej ☐

B8.) Kan man generera regler manuellt eller måste man starta varje applikation och låta brandväggen skapa reglerna?

Ja ☐ Nej ☐

C.) BRANDVÄGGSFUNKTIONER

C1.) Kontrollerar den ingående trafik?

Ja ☐ Nej ☐

C2.) Kontrollerar den utgående trafik?

Ja ☐ Nej ☐

C3.) Finns det någon stopp-funktion?

Ja ☐ Nej ☐

C4.) Finns det någon funktion för automatisk uppdatering?

Ja ☐ Nej ☐

C5.) Kan man tillåta att en applikation får tillgång till nätverket tillfälligt?

Ja ☐ Nej ☐

C6.) Kan man tillåta att en applikation alltid får tillgång till nätverket?

Ja ☐ Nej ☐

C7.) Kontrollerar brandväggen checksummor för godkända applikationer?

Ja ☐ Nej ☐

C8.) Kan man exportera/spara regellistor?

Ja ☐ Nej ☐

C9.) Kan man importera regellistor?

Ja ☐ Nej ☐

D.) AVINSTALLATION

D1.) Raderas alla inställningar?

Ja ☐ Nej ☐

E.) HJÄLPFUNKTIONER

E1.) Finns manual lätt tillgängligt?

Ja ☐ Nej ☐

E2.) Finns informationen på svenska?

Ja ☐ Nej ☐

Appendix C – Skannade portar (Blackcode)

Port	Service	Port	Service	Port	Service
1	tcpmux	2	compressnet	3	compressnet
5	rje	7	echo	9	discard
11	systat	13	daytime	17	qotd
18	msp	19	chargen	20	ftp-data
21	ftp	23	telnet	24	
25	smtp	27	nsw-fe	29	msg-icp
31	msg-auth	33	dsp	35	
37	time	38	rap	39	rlp
41	graphics	42	nameserver	43	nicname
44	mpm-flags	45	mpm	46	mpm-snd
47	ni-ftp	48	auditd	49	login
50	re-mail-ck	51	la-maint	52	xns-time
53	domain	54	xns-ch	55	isi-gl
56	xns-auth	57		58	xns-mail
59		61	ni-mail	62	acas
64	covia	65	tacacs-ds	66	sql*net
67	bootps	68	bootpc	69	tftp
70	gopher	71	netrjs-1	72	netrjs-2
73	netrjs-3	74	netrjs-4	75	
76	deos	77		78	vettcp
79	finger	80	www-http	81	hosts2-ns
82	xfer	83	mit-ml-dev	84	ctf
85	mit-ml-dev	86	mfcobol	87	
88	kerberos	89	su-mit-tg	90	dnsix
91	mit-dov	92	npp	93	dcp
94	objcall	95	supdup	96	dixie
97	swift-rvf	98	tacnews	99	metagram
100	newacct	101	hostname	102	iso-tsap
103	gppitnp	104	acr-nema	105	csnet-ns
106	3com-tsmux	107	rtelnet	108	snagas
109	pop2	110	pop3	111	sunrpc
112	mcidas	113	auth	114	audionews
115	sftp	116	ansanotify	117	uucp-path
118	sqlserv	119	nntp	120	cfdptkt
121	erpc	122	smakynet	123	ntp
124	ansatrader	125	locus-map	126	unitary
127	locus-con	128	gss-xlicen	129	pwdgen
130	cisco-fna	131	cisco-tna	132	cisco-sys
133	statsrv	134	ingres-net	135	loc-srv
136	profile	137	netbios-ns	138	netbios-dgm
139	netbios-ssn	140	emfis-data	141	emfis-cntl
142	bl-idm	143	imap2	144	news
145	uaac	146	iso-tp0	147	iso-ip
148	cronus	149	aed-512	150	sql-net
151	hems	152	bftp	153	sgmp
154	netsc-prod	155	netsc-dev	156	sqlsrv
157	knet-cmp	158	pcmail-srv	159	nss-routing
160	sgmp-traps	161	snmp	162	snmptrap
163	cmip-man	164	cmip-agent	165	xns-courier
166	s-net	167	namp	168	rsvd
169	send	170	print-srv	171	multiplex
172	cl/1	173	xyplex-mux	174	mailq
175	vmnet	176	genrad-mux	177	xdmcp
178	nextstep	179	bgp	180	ris
181	unify	182	audit	183	ocbinder

184	ocserver	185	remote-kis	186	kis
187	aci	188	mumps	189	qft
190	gacp	191	prospero	192	osu-nms
193	srmp	194	irc	195	dn6-nlm-aud
196	dn6-smm-red	197	dls	198	dls-mon
199	smux	200	src	201	at-rtmp
202	at-nbp	203	at-3	204	at-echo
205	at-5	206	at-zis	207	at-7
208	at-8	209	tam	210	z39.50
211	914c/g	212	anet	213	ipx
214	vmpwscs	215	softpc	216	atls
217	dbase	218	mpp	219	uarps
220	imap3	221	fln-spx	222	rsh-spx
223	cdc	243	sur-meas	245	link
246	dsp3270	344	pdap	345	pawserv
346	zserv	347	fatserv	348	csi-sgwp
371	clearcase	372	ulistserv	373	legent-1
374	legent-2	375	hassle	376	nip
377	tnETOS	378	dsETOS	379	is99c
380	is99s	381	hp-collector	382	hp-managed-node
383	hp-alarm-mgr	384	arns	385	ibm-app
386	asa	387	aurp	388	unidata-ldm
389	ldap	390	uis	391	synotics-relay
392	synotics-broker	393	dis	394	embl-ndt
395	netcp	396	netware-ip	397	mptn
398	kryptolan	400	work-sol	401	ups
402	genie	403	decap	404	nced
405	ncld	406	imsp	407	timbuktu
408	prm-sm	409	prm-nm	410	decladebug
411	rmt	412	synoptics-trap	413	smsp
414	infoseek	415	bnet	416	silverplatter
417	onmux	418	hyper-g	419	ariel1
420	smpte	421	ariel2	422	ariel3
423	opc-job-start	424	opc-job-track	425	icad-el
426	smartsdp	427	svrloc	428	ocs_cmu
429	ocs_amu	430	utmpsd	431	utmpcd
432	iasd	433	nnsp	434	mobileip-agent
435	mobilip-mn	436	dna-cml	437	comscm
438	dsfgw	439	dasp	440	sgcp
441	decvms-sysmgt	442	cvc_hostd	443	https
444	snpp	445	microsoft-ds	446	ddm-rdb
447	ddm-dfm	448	ddm-byte	449	as-servermap
450	tserver	512	exec	513	login
514	cmd	515	printer	517	talk
518	ntalk	519	utime	520	efs
525	timed	526	tempo	530	courier
531	conference	532	netnews	533	netwall
539	apertus-ldp	540	uucp	541	uucp-rlogin
543	klogin	544	kshell	550	new-rwho
555	dsf	556	remotefs	560	rmonitor
561	monitor	562	chshell	564	9pfs
565	whoami	570	meter	571	meter
600	ipcserver	606	urm	607	nqs
608	sift-uft	609	npmp-trap	610	npmp-local
611	npmp-gui	634	ginad	666	mdqs
704	elcsd	709	entrustmanager	729	netviewdm1

730	netviewdm2	731	netviewdm3	741	netgw
742	netrcs	744	flexlm	747	fujitsu-dev
748	ris-cm	749	kerberos-adm	750	rfile
751	pump	752	qrh	753	rrh
754	tell	758	nlogin	759	con
760	ns	761	rxe	762	quotad
763	cycleserv	764	omserv	765	webster
767	phonebook	769	vid	770	cadlock
771	rtip	772	cycleserv2	773	submit
774	rpasswd	775	entomb	776	wpages
780	wpgs	786	concert	800	mdbs_daemon
801	device	996	xtreelic	997	maitrd
998	busboy	999	garcon	1000	cadlock

Appendix D – ICSA kriterier

HOST PROTECTION AND FUNCTIONALITY

Microsoft Networking Compatibility Series (LAN only)

- System must be able to log into the MS test domain on the trusted LAN to access CIFS/Microsoft-RPC resources.
- Access to file/print services must function as prior to installation of the PCFW
- Ability to access UNC shares on the LAN without further configuration must be demonstrated.
- If the product requires confirmation in order to access MS domain resources, such confirmations must be persistent across system reboot

TCP/IP - Winsock - Arbitrary Client (LAN and Dialup)

- Using arbitrary (non commercial) client applications, an attempts will be made to access simple-single-port TCP and UDP servers, and thereafter to exchange data with that server.
- The product must prompt the user for permission before allowing the application to contact the server

TCP/IP - Winsock - Client Application Compatibility Series (LAN and Dialup)

- Applications of the network application software suite that are not CIFS/Microsoft
- RPC based will be tested for normal operation over both dialup and LAN networking.
- If the application requires confirmation to access resources, the confirmation must be persistent across system if the product requires confirmation in order to permit reboots.
- This test will address client functionality of the applications only. Default is to deny

TCP/IP - Winsock - Arbitrary Server (LAN and Dialup)

- Using arbitrary (non commercial) client applications, attempts will be made to activate simple-single-port TCP and UDP servers on the testing platform, and thereafter to permit client applications from arbitrary addresses access that server.
- The product must prompt the user for permission before allowing the application to be accessible by remote clients.

NETWORK PROTECTION AND FUNCTIONALITY

Trusted Network Server Protection and Functionality

- The product must be able to permit arbitrary network servers on the test platform to function normally, while preventing access-to or detection-of that service by remote systems.
- This functionality must be able to support both CIFS/MS-RPC applications (such as file sharing) and Winsock applications.
- This product must be able to provide this protection on either or both of the network interfaces.
- This behavior must be the default configuration of the product. [trojan defense]

Trusted Network Client Protection and Functionality

- The product must be able to permit arbitrary network clients on the test platform to function normally, while preventing that client from accessing the network
- This functionality must be able to support both CIFS/MS-RPC applications and Winsock applications.
- This product must be able to provide this protection on either or both of the network interfaces.
- This behavior must be the default configuration of the product. [trojan defense]

Untrusted Network Client Protection/Functionality

- The product must be able to protect the test platform, and protected services from access, while permitting client applications to function properly.
- The test platform must protect the test platform, and further must not reveal the existence of the active (but protected) services to remote systems on the untrusted network, while permitting client applications on the test platform to function normally

Untrusted Network Server Protection/Functionality

- Repeat test conditions above with following exceptions:
    - One TCP service is configured to be accessible from the untrusted network
    - One UDP service is configured to be accessible from the untrusted network
- The test platform must allow only the designated services to be accessible/detectable from the untrusted network while protecting all others from access/detection.

DYNAMIC ADDRESS TESTING

- Client and server tests will be repeated in both a DHCP LAN environment as well as across multiple concurrent dialup connections.
- Measures will be taken to ensure that DHCP issues new/different address leases to the system in the course of testing
- Various spoofing/probing attempts using previously assigned addresses
- Goal of testing is to establish that previously used addresses are not trusted, and that the currently assigned address(es) is appropriately protected.

CURRENT THREATS

- Network Attacks - Untrusted Network Client Protection Configuration
    - The candidate product must successfully protect the test platform and protected applications from commonly available network attacks and probes.
- Malicious code Attacks - "Full Blackout" Configuration
    - Applications in the test suite serve as clients only
    - Applications will be demonstrated to be functional
    - Currently prevalent "network active" malicious code will be installed on the system
    - The product must prevent malicious code from accessing the network.
    - Test will be repeated with LAN interface untrusted
    - Test will be repeated with both interfaces untrusted

LOGGING/REPORTING

- The candidate product must log attempts to access the test platform which are prohibited by the configuration (policy)
- Logged events shall include a date and time, protocol, source/destination IP address and port (or ICMP type etc.).

PRIVACY

- The candidate product shall demonstrate through both attestation and testing that no unauthorized access or modification of user-supplied information is permitted through the proper use of encryption, authentication and segmentation.
- The candidate product vendor must disclose the content, destination, and communication path used for any information that the product communicates via any means to any location other than the test platform's local storage.
- Vendor attestation is the primary means by which this criterion is met, however any substantiated indication that the product behaves otherwise will result in a de-certification of the product

Appendix E - Formulärsvar

	BI	ZA	ZAP	TPF	ICF	SPF
A1	JA	JA	JA	JA	NEJ	JA
A2	JA	JA	JA	JA	JA	JA
B1a	NEJ	NEJ	NEJ	JA	NEJ	JA
B1b	NEJ	NEJ	NEJ	JA	NEJ	JA
B2a	NEJ	NEJ	JA	JA	NEJ	JA
B2b	NEJ	NEJ	JA	JA	NEJ	JA
B3	JA	NEJ	JA	JA	JA	JA
B4	NEJ	NEJ	JA	NEJ	JA	NEJ
B5	NEJ	NEJ	JA	NEJ	JA	NEJ
B6	NEJ	NEJ	JA	JA	NEJ	NEJ
B7	NEJ	JA	JA	JA	NEJ	NEJ
B8	NEJ	NEJ	JA	JA	JA	JA
C1	JA	JA	JA	JA	JA	JA
C2	JA	JA	JA	JA	NEJ	JA
C3	NEJ	JA	JA	JA	NEJ	JA
C4	JA	JA	JA	JA	JA	JA
C5	JA	JA	JA	JA	NEJ	JA
C6	JA	JA	JA	JA	NEJ	JA
C7	NEJ	JA	JA	JA	NEJ	JA
C8	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ
C9	NEJ	NEJ	NEJ	NEJ	NEJ	NEJ
D1	JA	NEJ	NEJ	JA	JA	JA
E1	JA	Ja	Ja	NEJ	JA	JA
E2	NEJ	NEJ	NEJ	NEJ	JA	NEJ

BI = BlackICE PC Protection, Shareware
ZA = ZoneAlarm 2.6, Freeware
ZAP = ZoneAlarm PRO 3, Shareware
TPF = Tiny Personal Firewall, Freeware
ICF = Internet Connection Firewall, Medföljer Windows XP
SPF = Sygate Personal Firewall, Shareware

Appendix F - Testresultat

Test utan brandvägg

Shields UP! - Probe my ports

Port	Service	Status
21	FTP	Stängd
23	Telnet	Stängd
25	SMTP	Stängd
79	Finger	Stängd
110	POP3	Stängd
113	IDENT	Stängd
135	RPC	Öppen
139	NetBIOS	Öppen
143	IMAP	Stängd
443	HTTPS	Stängd
445	MSFT DS	Öppen
5000	UPnP	Öppen

Öppen Porten är open för anslutningar.
Stängd Datorn visar att porten finns, men den är stängd och accepterar inte anslutningar.
Gömd Porten syns inte alls utifrån.

Sygate Quick Scan

Portscan

Ports	Service	Status
20	FTP Data	Stängd
21	FTP	Stängd
22	SSH	Stängd
23	Telnet	Stängd
25	SMTP	Stängd
53	DNS	Stängd
59	DDC	Stängd
79	Finger	Stängd
80	Web	Stängd
110	POP3	Stängd
113	IDENT	Stängd
135	Location Service	Öppen
139	NetBIOS	Öppen
443	HTTPS	Stängd
445	Server Message Block	Öppen
1080	Socks Proxy	Stängd
5000	UPnP	Öppen
8080	Web Proxy	Stängd

Commonly used Trojans scan

Ports	Status	Trojaner som använder denna port
1243	Stängd	BackDoor-G, SubSeven, SubSeven Apocalypse
1999	Stängd	BackDoor, TtansScout
6776	Stängd	BackDoor-G, SubSeven
7789	Stängd	Back Door Setup, ICKiller
12345	Stängd	GabanBus, NetBus, Pie Bill Gates, X-bill
31337	Stängd	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO
54320	Stängd	Back Orifice 2000
54321	Stängd	School Bus, Back Orifice 2000

BLACKCODE

Well Known Port Numbers Scan

Ports	Service	Status
135	loc-srv	Öppen
139	netbios-ssn	Öppen
445	microsoft-ds	Öppen

Trojan Horse Scan

Ports	Status	Trojaner som använder denna port
139	Öppen	Chode, God Message worm, Msinit, Netlog, Network, Qaz
1025	Öppen	Remote Storm
5000	Öppen	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie

SecurityMetrics

Port Scan

Ports	Service	Status
21	FTP	Stängd
22	SSH	Stängd
23	Telnet	Stängd
25	SMTP	Stängd
53	DNS	Stängd
59	IDENT	Stängd
79	Finger	Stängd
80	HTTP	Stängd
110	POP3	Stängd
139	NetBIOS	Öppen
161	SNMP	Stängd
443	SSL	Stängd
445	MS DS	Öppen
1080	SOCKS Proxy	Stängd
5000	UPnP	Öppen
8080	HTTP Proxy	Stängd

Trojan Port Scan

Port	Status	Trojaner som använder denna port
6776	Stängd	2000 Cracks, BackDoor-G, SubSeven, VP Killer
7000	Stängd	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
12345	Stängd	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill
20034	Stängd	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
27374	Stängd	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader
31337	Stängd	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini

Test av BlackICE PC Protection version 3.5.cbfE

Shields UP! - Probe my ports

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Port	**Service**	**Status**	**Status**	**Status**	**Status**
21	FTP	Stängd	Gömd	Gömd	Gömd
23	Telnet	Stängd	Gömd	Gömd	Gömd
25	SMTP	Stängd	Gömd	Gömd	Gömd
79	Finger	Stängd	Gömd	Gömd	Gömd
110	POP3	Stängd	Gömd	Gömd	Gömd
113	IDENT	Stängd	Stängd	Stängd	Stängd
135	RPC	Öppen	Gömd	Gömd	Gömd
139	NetBIOS	Gömd	Gömd	Gömd	Gömd
143	IMAP	Stängd	Gömd	Gömd	Gömd
443	HTTPS	Stängd	Gömd	Gömd	Gömd
445	MSFT DS	Gömd	Gömd	Gömd	Gömd
5000	UPnP	Öppen	Öppen	Gömd	Gömd

Sygate Quick Scan

Portscan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Ports	**Service**	**Status**	**Status**	**Status**	**Status**
20	FTP Data	Stängd	Gömd	Gömd	Gömd
21	FTP	Stängd	Gömd	Gömd	Gömd
22	SSH	Stängd	Gömd	Gömd	Gömd
23	Telnet	Stängd	Gömd	Gömd	Gömd
25	SMTP	Stängd	Gömd	Gömd	Gömd
53	DNS	Stängd	Gömd	Gömd	Gömd
59	DDC	Stängd	Gömd	Gömd	Gömd
79	Finger	Stängd	Gömd	Gömd	Gömd
80	Web	Stängd	Stängd	Stängd	Stängd
110	POP3	Stängd	Gömd	Gömd	Gömd
113	IDENT	Stängd	Stängd	Stängd	Stängd
135	Location Service	Öppen	Gömd	Gömd	Gömd
139	NetBIOS	Gömd	Gömd	Gömd	Gömd
443	HTTPS	Stängd	Gömd	Gömd	Gömd
445	Server Message Block	Gömd	Gömd	Gömd	Gömd
1080	Socks Proxy	Stängd	Stängd	Gömd	Gömd
5000	UPnP	Öppen	Öppen	Gömd	Gömd
8080	Web Proxy	Stängd	Stängd	Gömd	Gömd

Commonly used Trojans scan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**	**Status**
1243	BackDoor-G, SubSeven, SubSeven Apocalypse	Stängd	Stängd	Gömd	Gömd
1999	BackDoor, TtansScout	Stängd	Stängd	Gömd	Gömd
6776	BackDoor-G, SubSeven	Stängd	Stängd	Gömd	Gömd
7789	Back Door Setup, ICKiller	Stängd	Stängd	Gömd	Gömd
12345	GabanBus, NetBus, Pie Bill Gates, X-bill	Stängd	Stängd	Gömd	Gömd
31337	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	Stängd	Stängd	Gömd	Gömd
54320	Back Orifice 2000	Stängd	Stängd	Gömd	Gömd
54321	School Bus, Back Orifice 2000	Stängd	Stängd	Gömd	Gömd

BLACKCODE

Well Known Port Numbers Scan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Ports	**Service**	**Status**	**Status**	**Status**	**Status**
135	loc-srv	Öppen	Closed	Closed	Closed

Trojan Horse Scan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**	**Status**
1025	Remote Storm	Öppen	Öppen	Closed	Closed
5000	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie	Öppen	Öppen	Closed	Closed

SecurityMetrics

Port Scan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Ports	**Service**	**Status**	**Status**	**Status**	**Status**
21	FTP	Stängd	Gömd	Gömd	Gömd
22	SSH	Stängd	Gömd	Gömd	Gömd
23	Telnet	Stängd	Gömd	Gömd	Gömd
25	SMTP	Stängd	Gömd	Gömd	Gömd
53	DNS	Stängd	Gömd	Gömd	Gömd
59	IDENT	Stängd	Gömd	Gömd	Gömd
79	Finger	Stängd	Gömd	Gömd	Gömd
80	HTTP	Stängd	Gömd	Gömd	Gömd
110	POP3	Stängd	Gömd	Gömd	Gömd
139	NetBIOS	Gömd	Gömd	Gömd	Gömd
161	SNMP	Stängd	Gömd	Gömd	Gömd
443	SSL	Stängd	Gömd	Gömd	Gömd
445	MS DS	Gömd	Gömd	Gömd	Gömd
1080	SOCKS Proxy	Stängd	Stängd	Gömd	Gömd
5000	UPnP	Öppen	Öppen	Gömd	Gömd
8080	HTTP Proxy	Stängd	Stängd	Gömd	Gömd

Trojan Port Scan

		Trusting	*Cautious*	*Nervous*	*Paranoid*
Port	**Trojaner som använder denna port**	**Status**	**Status**	**Status**	**Status**
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer	Stängd	Stängd	Gömd	Gömd
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold	Stängd	Stängd	Gömd	Gömd
12345	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill	Stängd	Stängd	Gömd	Gömd
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job	Stängd	Stängd	Gömd	Gömd
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader	Stängd	Stängd	Gömd	Gömd
31337	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini	Stängd	Stängd	Gömd	Gömd

Test av Sygate Personal Firewall 5.0

Shields UP! - Probe my ports

		Allow all	*Normal*	*Block all*
Port	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Gömd	N/A
23	Telnet	Stängd	Gömd	N/A
25	SMTP	Stängd	Gömd	N/A
79	Finger	Stängd	Gömd	N/A
110	POP3	Stängd	Gömd	N/A
113	IDENT	Stängd	Stängd	N/A
135	RPC	Gömd	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
143	IMAP	Stängd	Gömd	N/A
443	HTTPS	Stängd	Gömd	N/A
445	MSFT DS	Gömd	Gömd	N/A
5000	UPnP	Öppen	Gömd	N/A

Sygate Quick Scan

Portscan

		Allow all	*Normal*	*Block all*
Ports	**Service**	**Status**	**Status**	**Status**
20	FTP Data	Stängd	Gömd	N/A
21	FTP	Stängd	Gömd	N/A
22	SSH	Stängd	Gömd	N/A
23	Telnet	Stängd	Gömd	N/A
25	SMTP	Stängd	Gömd	N/A
53	DNS	Stängd	Gömd	N/A
59	DDC	Stängd	Gömd	N/A
79	Finger	Stängd	Gömd	N/A
80	Web	Stängd	Stängd	N/A
110	POP3	Stängd	Gömd	N/A
113	IDENT	Stängd	Stängd	N/A
135	Location Service	Gömd	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
443	HTTPS	Stängd	Gömd	N/A
445	Server Message Block	Gömd	Gömd	N/A
1080	Socks Proxy	Stängd	Gömd	N/A
5000	UPnP	Öppen	Gömd	
8080	Web Proxy	Stängd	Gömd	N/A

Commonly used Trojans scan

		Allow all	*Normal*	*Block all*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1243	BackDoor-G, SubSeven, SubSeven Apocalypse	Stängd	Gömd	N/A
1999	BackDoor, TtansScout	Stängd	Gömd	N/A
6776	BackDoor-G, SubSeven	Stängd	Gömd	N/A
7789	Back Door Setup, ICKiller	Stängd	Gömd	N/A
12345	GabanBus, NetBus, Pie Bill Gates, X-bill	Stängd	Gömd	N/A
31337	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	Stängd	Gömd	N/A
54320	Back Orifice 2000	Stängd	Gömd	N/A
54321	School Bus, Back Orifice 2000	Stängd	Gömd	N/A

BLACKCODE

Well Known Port Numbers Scan

Alla portar stängda.

Trojan Horse Scan

		Allow all	*Normal*	*Block all*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1025	Remote Storm	Öppen	Stängd	N/A
5000	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie	Öppen	Stängd	N/A

SecurityMetrics

Port Scan

		Allow all	*Normal*	*Block all*
Ports	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Gömd	N/A
22	SSH	Stängd	Gömd	N/A
23	Telnet	Stängd	Gömd	N/A
25	SMTP	Stängd	Gömd	N/A
53	DNS	Stängd	Gömd	N/A
59	IDENT	Stängd	Gömd	N/A
79	Finger	Stängd	Gömd	N/A
80	HTTP	Stängd	Gömd	N/A
110	POP3	Stängd	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
161	SNMP	Stängd	Gömd	N/A
443	SSL	Stängd	Gömd	N/A
445	MS DS	Gömd	Gömd	N/A
1080	SOCKS Proxy	Stängd	Gömd	N/A
5000	UPnP	Öppen	Gömd	N/A
8080	HTTP Proxy	Stängd	Gömd	N/A

Trojan Port Scan

		Allow all	*Normal*	*Block all*
Port	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer	Stängd	Gömd	N/A
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold	Stängd	Gömd	N/A
12345	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill	Stängd	Gömd	N/A
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job	Stängd	Gömd	N/A
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader	Stängd	Gömd	N/A
31337	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini	Stängd	Gömd	N/A

Test av Tiny Personal Firewall – 2.0.15 A (221001)

Shields UP! - Probe my ports

		Don't bother me	*Ask me first*	*Cut me off*
Port	**Service**	**Status**	**Status**	**Status**
21	FTP	Gömd	Gömd	N/A
23	Telnet	Gömd	Gömd	N/A
25	SMTP	Gömd	Gömd	N/A
79	Finger	Gömd	Gömd	N/A
110	POP3	Gömd	Gömd	N/A
113	IDENT	Stängd	Stängd	N/A
135	RPC	Öppen	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
143	IMAP	Gömd	Gömd	N/A
443	HTTPS	Gömd	Gömd	N/A
445	MSFT DS	Gömd	Gömd	N/A
5000	UPnP	Öppen	Gömd	N/A

Sygate Quick Scan

Portscan

		Don't bother me	*Ask me first*	*Cut me off*
Ports	**Service**	**Status**	**Status**	**Status**
20	FTP Data	Gömd	Gömd	N/A
21	FTP	Gömd	Gömd	N/A
22	SSH	Gömd	Gömd	N/A
23	Telnet	Gömd	Gömd	N/A
25	SMTP	Gömd	Gömd	N/A
53	DNS	Gömd	Gömd	N/A
59	DDC	Gömd	Gömd	N/A
79	Finger	Gömd	Gömd	N/A
80	Web	Stängd	Stängd	N/A
110	POP3	Gömd	Gömd	N/A
113	IDENT	Stängd	Stängd	N/A
135	Location Service	Öppen	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
443	HTTPS	Gömd	Gömd	N/A
445	Server Message Block	Gömd	Gömd	N/A
1080	Socks Proxy	Gömd	Gömd	N/A
5000	UPnP	Öppen	Gömd	
8080	Web Proxy	Gömd	Gömd	N/A

Commonly used Trojans scan

		Don't bother me	*Ask me first*	*Cut me off*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1243	BackDoor-G, SubSeven, SubSeven Apocalypse	Gömd	Gömd	N/A
1999	BackDoor, TtansScout	Gömd	Gömd	N/A
6776	BackDoor-G, SubSeven	Gömd	Gömd	N/A
7789	Back Door Setup, ICKiller	Gömd	Gömd	N/A
12345	GabanBus, NetBus, Pie Bill Gates, X-bill	Gömd	Gömd	N/A
31337	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	Gömd	Gömd	N/A
54320	Back Orifice 2000	Gömd	Gömd	N/A
54321	School Bus, Back Orifice 2000	Gömd	Gömd	N/A

BLACKCODE

Well Known Port Numbers Scan

		Don't bother me	*Ask me first*	*Cut me off*
Ports	**Service**	**Status**	**Status**	**Status**
135	loc-srv	Öppen	Stängd	N/A

Trojan Horse Scan

		Don't bother me	*Ask me first*	*Cut me off*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1025	Remote Storm	Öppen	Stängd	N/A
5000	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie	Öppen	Stängd	N/A

SecurityMetrics

Port Scan

		Don't bother me	*Ask me first*	*Cut me off*
Ports	**Service**	**Status**	**Status**	**Status**
21	FTP	Gömd	Gömd	N/A
22	SSH	Gömd	Gömd	N/A
23	Telnet	Gömd	Gömd	N/A
25	SMTP	Gömd	Gömd	N/A
53	DNS	Gömd	Gömd	N/A
59	IDENT	Gömd	Gömd	N/A
79	Finger	Gömd	Gömd	N/A
80	HTTP	Gömd	Gömd	N/A
110	POP3	Gömd	Gömd	N/A
139	NetBIOS	Gömd	Gömd	N/A
161	SNMP	Gömd	Gömd	N/A
443	SSL	Gömd	Gömd	N/A
445	MS DS	Gömd	Gömd	N/A
1080	SOCKS Proxy	Gömd	Gömd	N/A
5000	UPnP	Öppen	Gömd	N/A
8080	HTTP Proxy	Gömd	Gömd	N/A

Trojan Port Scan

		Don't bother me	*Ask me first*	*Cut me off*
Port	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer	Gömd	Gömd	N/A
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold	Gömd	Gömd	N/A
12345	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill	Gömd	Gömd	N/A
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job	Gömd	Gömd	N/A
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader	Gömd	Gömd	N/A
31337	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini	Gömd	Gömd	N/A

Test av Internet Connection Firewall

Shields UP! - Probe my ports

Port	Service	Status
21	FTP	Gömd
23	Telnet	Gömd
25	SMTP	Gömd
79	Finger	Gömd
110	POP3	Gömd
113	IDENT	Stängd
135	RPC	Gömd
139	NetBIOS	Gömd
143	IMAP	Gömd
443	HTTPS	Gömd
445	MSFT DS	Gömd
5000	UPnP	Gömd

Sygate Quick Scan

Portscan

Ports	Service	Status
20	FTP Data	Gömd
21	FTP	Gömd
22	SSH	Gömd
23	Telnet	Gömd
25	SMTP	Gömd
53	DNS	Gömd
59	DDC	Gömd
79	Finger	Gömd
80	Web	Stängd
110	POP3	Gömd
113	IDENT	Stängd
135	Location Service	Gömd
139	NetBIOS	Gömd
443	HTTPS	Gömd
445	Server Message Block	Gömd
1080	Socks Proxy	Gömd
5000	UPnP	Gömd
8080	Web Proxy	Gömd

Commonly used Trojans scan

Ports	Status	Trojaner som använder denna port
1243	Gömd	BackDoor-G, SubSeven, SubSeven Apocalypse
1999	Gömd	BackDoor, TtansScout
6776	Gömd	BackDoor-G, SubSeven
7789	Gömd	Back Door Setup, ICKiller
12345	Gömd	GabanBus, NetBus, Pie Bill Gates, X-bill
31337	Gömd	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO
54320	Gömd	Back Orifice 2000
54321	Gömd	School Bus, Back Orifice 2000

BLACKCODE

Well Known Port Numbers Scan

Alla portar stängda.

Trojan Horse Scan

Inga av de portar som de vanligaste trojanerna använder sig av är öppna.

SecurityMetrics

Port Scan

Ports	Service	Status
21	FTP	Gömd
22	SSH	Gömd
23	Telnet	Gömd
25	SMTP	Gömd
53	DNS	Gömd
59	IDENT	Gömd
79	Finger	Gömd
80	HTTP	Gömd
110	POP3	Gömd
139	NetBIOS	Gömd
161	SNMP	Gömd
443	SSL	Gömd
445	MS DS	Gömd
1080	SOCKS Proxy	Gömd
5000	UPnP	Gömd
8080	HTTP Proxy	Gömd

Trojan Port Scan

Port	Status	Trojaner som använder denna port
6776	Gömd	2000 Cracks, BackDoor-G, SubSeven, VP Killer
7000	Gömd	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
12345	Gömd	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill
20034	Gömd	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
27374	Gömd	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader
31337	Gömd	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini

Test av ZoneAlarm 2.6

Shields UP! - Probe my ports

		Low	*Medium*	*High*
Port	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
110	POP3	Stängd	Stängd	Gömd
113	IDENT	Stängd	Stängd	Stängd
135	RPC	Öppen	Gömd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
143	IMAP	Stängd	Stängd	Gömd
443	HTTPS	Stängd	Stängd	Gömd
445	MSFT DS	Öppen	Gömd	Gömd
5000	UPnP	Öppen	Öppen	Gömd

Sygate Quick Scan & Gömd Scan

Portscan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
20	FTP Data	Stängd	Stängd	Gömd
21	FTP	Stängd	Stängd	Gömd
22	SSH	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
53	DNS	Stängd	Stängd	Gömd
59	DDC	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
80	Web	Stängd	Stängd	Stängd
110	POP3	Stängd	Stängd	Gömd
113	IDENT	Stängd	Stängd	Stängd
135	Location Service	Öppen	Gömd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
443	HTTPS	Stängd	Stängd	Gömd
445	Server Message Block	Öppen	Gömd	Gömd
1080	Socks Proxy	Stängd	Stängd	Gömd
5000	UPnP	Öppen	Öppen	Gömd
8080	Web Proxy	Stängd	Stängd	Gömd

Commonly used Trojans scan

		Low	*Medium*	*High*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1243	BackDoor-G, SubSeven, SubSeven Apocalypse	Stängd	Stängd	Gömd
1999	BackDoor, TtansScout	Stängd	Stängd	Gömd
6776	BackDoor-G, SubSeven	Stängd	Stängd	Gömd
7789	Back Door Setup, ICKiller	Stängd	Stängd	Gömd
12345	GabanBus, NetBus, Pie Bill Gates, X-bill	Stängd	Stängd	Gömd
31337	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	Stängd	Stängd	Gömd
54320	Back Orifice 2000	Stängd	Stängd	Gömd
54321	School Bus, Back Orifice 2000	Stängd	Stängd	Gömd

BLACKCODE

Well Known Port Numbers Scan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
135	loc-srv	Öppen	Stängd	Stängd
139	netbios-ssn	Öppen	Stängd	Stängd
445	microsoft-ds	Öppen	Stängd	Stängd

Trojan Horse Scan

		Low	*Medium*	*High*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
139	Chode, God Message worm, Msinit, Netlog, Network, Qaz	Öppen	Stängd	Stängd
1025	Remote Storm	Öppen	Öppen	Stängd
5000	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie	Öppen	Öppen	Stängd

SecurityMetrics

Port Scan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Stängd	Gömd
22	SSH	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
53	DNS	Stängd	Stängd	Gömd
59	IDENT	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
80	HTTP	Stängd	Stängd	Gömd
110	POP3	Stängd	Stängd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
161	SNMP	Stängd	Stängd	Gömd
443	SSL	Stängd	Stängd	Gömd
445	MS DS	Öppen	Gömd	Gömd
1080	SOCKS Proxy	Stängd	Stängd	Gömd
5000	UPnP	Öppen	Öppen	Gömd
8080	HTTP Proxy	Stängd	Stängd	Gömd

Trojan Port Scan

		Low	*Medium*	*High*
Port	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer	Stängd	Stängd	Gömd
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold	Stängd	Stängd	Gömd
12345	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill	Stängd	Stängd	Gömd
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job	Stängd	Stängd	Gömd
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader	Stängd	Stängd	Gömd
31337	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini	Stängd	Stängd	Gömd

Test av ZoneAlarm PRO 3

Shields UP! - Probe my ports

		Low	*Medium*	*High*
Port	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
110	POP3	Stängd	Stängd	Gömd
113	IDENT	Stängd	Stängd	Stängd
135	RPC	Öppen	Gömd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
143	IMAP	Stängd	Stängd	Gömd
443	HTTPS	Stängd	Stängd	Gömd
445	MSFT DS	Öppen	Gömd	Gömd
5000	UPnP	Öppen	Öppen	Gömd

Sygate Quick Scan

Portscan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
20	FTP Data	Stängd	Stängd	Gömd
21	FTP	Stängd	Stängd	Gömd
22	SSH	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
53	DNS	Stängd	Stängd	Gömd
59	DDC	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
80	Web	Stängd	Stängd	Stängd
110	POP3	Stängd	Stängd	Gömd
113	IDENT	Stängd	Stängd	Stängd
135	Location Service	Öppen	Gömd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
443	HTTPS	Stängd	Stängd	Gömd
445	Server Message Block	Öppen	Gömd	Gömd
1080	Socks Proxy	Stängd	Stängd	Gömd
5000	UPnP	Öppen	Öppen	Gömd
8080	Web Proxy	Stängd	Stängd	Gömd

Commonly used Trojans scan

		Low	*Medium*	*High*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
1243	BackDoor-G, SubSeven, SubSeven Apocalypse	Stängd	Stängd	Gömd
1999	BackDoor, TtansScout	Stängd	Stängd	Gömd
6776	BackDoor-G, SubSeven	Stängd	Stängd	Gömd
7789	Back Door Setup, ICKiller	Stängd	Stängd	Gömd
12345	GabanBus, NetBus, Pie Bill Gates, X-bill	Stängd	Stängd	Gömd
31337	Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	Stängd	Stängd	Gömd
54320	Back Orifice 2000	Stängd	Stängd	Gömd
54321	School Bus, Back Orifice 2000	Stängd	Stängd	Gömd

BLACKCODE

Well Known Port Numbers Scan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
135	loc-srv	Öppen	Stängd	Stängd
139	netbios-ssn	Öppen	Stängd	Stängd
445	microsoft-ds	Öppen	Stängd	Stängd

Trojan Horse Scan

		Low	*Medium*	*High*
Ports	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
139	Chode, God Message worm, Msinit, Netlog, Network, Qaz	Öppen	Stängd	Stängd
1025	Remote Storm	Öppen	Öppen	Stängd
5000	Black Door Setup, Blazer5, Bubbel, ICKiller, Rald, Sockets des Troie	Öppen	Öppen	Stängd

SecurityMetrics

Port Scan

		Low	*Medium*	*High*
Ports	**Service**	**Status**	**Status**	**Status**
21	FTP	Stängd	Stängd	Gömd
22	SSH	Stängd	Stängd	Gömd
23	Telnet	Stängd	Stängd	Gömd
25	SMTP	Stängd	Stängd	Gömd
53	DNS	Stängd	Stängd	Gömd
59	IDENT	Stängd	Stängd	Gömd
79	Finger	Stängd	Stängd	Gömd
80	HTTP	Stängd	Stängd	Gömd
110	POP3	Stängd	Stängd	Gömd
139	NetBIOS	Öppen	Gömd	Gömd
161	SNMP	Stängd	Stängd	Gömd
443	SSL	Stängd	Stängd	Gömd
445	MS DS	Öppen	Gömd	Gömd
1080	SOCKS Proxy	Stängd	Stängd	Gömd
5000	UPnP	Öppen	Öppen	Gömd
8080	HTTP Proxy	Stängd	Stängd	Gömd

Trojan Port Scan

		Low	*Medium*	*High*
Port	**Trojaner som använder denna port**	**Status**	**Status**	**Status**
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer	Stängd	Stängd	Gömd
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven	Stängd	Stängd	Gömd
12345	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill	Stängd	Stängd	Gömd
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job	Stängd	Stängd	Gömd
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader	Stängd	Stängd	Gömd
31337	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockd.	Stängd	Stängd	Gömd