Filosofie kandidatuppsats inom datavetenskap 10 poäng i Informationssystem programmet
Institutionen för Programvaruteknik och Datavetenskap
Blekinge Tekniska Högskola

Juni 2003

En studie av inbyggda brandväggar
Microsoft XP & Red Hat Linux.

Författare
Johan Ahlgren
Robert Karlsson

Handledare
Anders Carlsson

Examinator
Guohua Bai

"I have not failed. I've just found 10,000 ways that won't work."
Thomas Alva Edison (1847-1931)

ABSTRACT

This theses investigates how two operatingsystems built-in firewalls work together with the most common services that people use on the Internet, and how similar they are in the way they act against the threats that exists there. The two operatingsystems in question are Microsoft Windows XP and Red Hat Linux 8.0.

The hypothesis that was used in this study is as follows: *The two built-in firewalls are basicly equal regarding protection from threats on the Internet and fullfills the users need for online services*. To answer the questions this thesis is based on, we used a method consisting of two tests. One functionality test, where we tested the most common services found on the Internet, and how well the built-in firewall handled these. The other one was a securitytest where both built-in firewalls where scanned and put through several vulnerability tests by the use of a variety of tools.

By analyzing our result we could see that both built-in firewalls does not interfere with the most common services found on the Internet. However a difference between them can be found regarding their exposure. Windows XPs built-in firewall is completly invisible from the outside, while the Linux firewall is not. From the Red Hat Linux built-in firewall, were we able to collect information from the host that potentially could, if fallen into the wrong hands, harm the system. We came to the conclusion that our hypothesis were to be falsified due to the fact that the two firewalls were not equal in terms of protection against external threats.

Keywords: firewall, operatingsystem, Linux, Windows, security, TCP/IP, scanning, XP, RedHat.

SAMMANFATTNING

Detta kandidatarbete utreder hur väl två operativsystems inbyggda brandväggar fungerar i symbios med en användares vanligaste tjänsteutnyttjande på Internet, samt att se hur likartade de är i sitt skydd från hot. De två operativsystemen som vi utgick ifrån var Microsoft Windows XP samt Red Hat Linux 8.0.

Den hypotes vi arbetat kring lyder enligt följande: *De två inbyggda brandväggarna är i stort likartade rörande skydd från hot på Internet och uppfyller användarnas tjänsteutnyttjande.* De metoder vi använt, för att svara på vår frågeställning, har delats upp i ett funktionalitetstest och ett säkerhetstest. I funktionalitetstestet provades de vanligaste Internettjänsterna med den inbyggda brandväggen och ifall det uppstod några komplikationer eller ej. De två inbyggda brandväggarna genom gick i säkerhetstestet skannings- och svaghetskontroll via ett flertal verktyg.

Genom resultatet kan vi konstatera att de inbyggda brandväggarna klarar av de vanligaste tjänsterna på Internet, men att en skillnad föreligger hos dem vad gäller exponeringen ut mot Internet. Windows XP ligger helt osynligt utåt, medan Red Hats inbyggda brandvägg avslöjar en mängd information om värddatorn, som kan komma att användas i illvilliga syften. Slutsatsen blev att vi avslutningsvis falsifierade vår hypotes då de två inbyggda brandväggarna ej var jämlika i sitt skydd mot yttre hot på Internet.

nyckelord : brandvägg, operativsystem, Linux, Windows, säkerhet, TCP/IP, skanning, XP, RedHat

Juni 2003

INNEHÅLLSFÖRTECKNING

1 INLEDNING

Säkerhetstänkandet för att skydda sin dator hos den vanlige användaren har med Internets större inflytande i våra liv, börjat breda ut sig allt mer. Ord som brandvägg, säkerhetsbugg, operativsystem, IP, trojan, hacker och så vidare, har även det tagit sin rot hos användaren, om än att många fortfarande är osäkra på vad som egentligen döljer sig bakom dessa begrepp.

Risken att utsättas för någon form av intrång, virus, trojan eller annan skada har drastiskt ökat i och med att tillgången till Internet med fast uppkoppling blivit allt vanligare. Hotet är allt från hackers, skript kids, men än oftare virus, spy-ware eller trojaner som användaren själv installerat i god tro. Företag, organisationer och till och med länder har genom brandväggar försökt skydda sig mot dessa hot.

Under de senare åren har även personliga brandväggar blivit en allt vanligare mjukvara att installera på sin dator som skydd mot inkräktare. Nu finns det även brandväggar direkt inbyggda i två av de populäraste operativsystemen från mjukvaruföretagen Microsoft och Red Hat.

När Microsoft 2001 släppte sitt nya operativsystem Windows XP hade de för första gången en fullständigt inbyggd brandvägg i sitt system. Microsofts operativsystem står idag för majoriteten av persondatorernas operativsystem och XP tar en allt större del av den marknaden [17]. Detta på grund av att Windowsanvändare och företag uppgraderar sina system eller köper nya datorer med XP som operativsystem.

Red Hat, den ledande distributören av operativsystemet Linux, har sedan version 7.0 också haft en inbyggd brandvägg som ett skydd mot intrång [16].

I kapitel 1 läggs grunden för detta arbete, där bland annat frågeställningen och hypotesen tas upp, dessa ska prägla detta kandidatarbetet. Detta följs upp med ett metodavsnitt följt av en bakgrund till hela ämnet i kapitel 3. Därefter följer upplägget för testerna och de verktyg som använts, samt hur de testerna genomförts. I kapitel 5 presenteras resultatet och diskuteras därefter i kapitel 6 där frågeställningen blir besvarad. Slutligen i kapitel 7 verifieras eller falsifieras hypotesen, följt av kapitel om egna reflektioner på vår insats och vidare utveckling kring ämnet, källor, samt appendix med bilagor av resultaten.

1.1 Problemområde

Varje gång en användare kopplar upp sig mot Internet utsätter han sin dator för exponering. Denna exponering innebär en risk att utsättas för intrångsförsök, resursutnyttjande, virus, trojaner, eller något av de andra hoten som finns ute på Internet. Olika operativsystem och applikationer medför skilda former av hot och risker. Särskilt datorer med Microsoft produkter, främst operativsystemet Windows och webbläsaren Internet Explorer, har varit utsatta för kontinuerliga säkerhetshål, som i sig bidragit till intrång och andra problem.

Ett sätt att skydda sig mot dessa hot är att använda sig av en mjukvarubrandvägg. Att använda sig av en brandvägg kan dels ge ett visst skydd, men även skapa en falsk säkerhet hos användaren. Det är inte alltid en brandvägg håller vad den lovar [26].

En brandvägg skall vara enkel att använda och konfigurera, den skall fungera tillsammans med andra applikationer som finns på datorn utan att för den delen skala av säkerheten mer än nödvändigt. Idag används de flesta datorerna till att surfa, hämta/skicka sin e-post, spela och någon form av Instant Message (IM) över Internet [27]. Dessa tjänster skall kunna fungera utan att brandväggen ska skapa komplikationer. Om en brandvägg medför att många, eller till och med vissa av de vanligaste applikationerna man använder sig av inte fungerar, är den absoluta risken att brandväggen blir frånkopplad av användaren. En svårkonfigurerad eller märkbar brandvägg kan komma att leda till sämre skydd och lider av större risk att kopplas ner.

1.2 Beroende och oberoende variabler

Säkerheten och funktionalitet står i beroende till varandra. Utan säkerhet uppfyller inte brandväggen sitt krav att skydda, men en brandvägg behöver även kunna fungera tillsammans med andra applikationer eller vara konfigurerbar mot dem.

1.3 Definition

Det finns olika former av brandväggar, och det är viktigt att skilja dem åt. När det talas om brandvägg i detta arbetet, menas en bred definition på alla olika typer av brandvägg. I detta arbete används definitionen *inbyggd brandvägg* för de fördefinierade och installerade brandväggar som ingår i operativtsystemet. Vid benämningen *användare* syftar detta till utnyttjaren av operativsystemet och/eller datorn. *Tjänsteutnyttjande* syftar på användandet av de vanligaste tjänsterna på Internet [27].

1.4 Hypotes

Vår hypotes vi arbetat utifrån under denna kandidatuppsats och har för syfte att falsifiera eller verifiera, lyder enligt följande:

”*De två inbyggda brandväggarna är i stort likartade rörande skydd från hot på Internet och uppfyller användarnas tjänsteutnyttjande.*”

1.5 Frågeställning

Följande frågeställningar står som grund för denna uppsats:

- *Hur klarar den inbyggda brandväggen av de vanligaste Internettjänsterna som användarna utnyttjar?*
- *Vad skiljer det två inbyggda brandväggarna åt ur ett operativt perspektiv?*
- *Vilka styrkor och svagheter finns det med respektive inbyggd brandvägg?*

Operativt perspektiv syftar på den rent tekniska aspekten av de inbyggda brandväggarna.

1.6 Syfte

Syftet är att jämföra och analysera Microsoft Windows XPs inbyggda brandvägg och Red Hat Linux 8.0s inbyggda brandvägg. En aspekt som kommer att tas i beaktning är att gå närmare in på de två inbyggda brandväggarna och fördjupa oss i flera valda delar. De delar som kommer att beröras innefattar säkerhetsaspekten, konfiguration och installation, samt funktionalitet mot de vanligaste tjänsterna som utnyttjas av användarna över Internet.

1.7 Mål

Målet är att genom en empirisk undersökning med säkerhetstester och funktionalitetstester, samt analys av respektive inbyggd brandvägg, presentera vårt resultat. Att genom utvalda applikationsverktyg, visa på skillnader och likheter samt visa hur de arbetar mot inkommande och utgående trafik. Det kommer även visa sig hur mycket skydd inbyggda brandväggar verkligen står för. I slutsatsen kommer hypotesen falsifieras eller verifieras.

1.8 Målgrupper

Denna kandidatuppsats sträcker sig främst till personer med ett gediget intresse för säkerhet, men likaså till studenter inom data- och systemvetenskapliga studier.

1.9 Avgränsning

Avgränsningen består i att inte beröra fel och säkerhetsbrister som plågar de två operativsystemen, här inkluderat virus och maskar som påverkas av operativsystemet.

Installationen, konfigurationen, funktionalitet och säkerheten av respektive nämnd inbyggd brandvägg kommer att beröras i arbetet. Vad gäller installation och konfigurering av brandväggarna kommer värderingen att utgå från ett rent tekniskt perspektiv och ej falla inom en kvalitativ undersökning. Detta medför att de inbyggda brandväggarnas användarvänlighet ej kommer att värderas.

Inga andra typer av brandväggar skall jämföras i denna uppsats.

2 METOD

Här presenteras de metoder som använts i framtagandet och bearbetandet av vårt resultat. Först i kapitel 4 kommer undersökningen att beröras mer ingående samt de verktyg som används för att studera de inbyggda brandväggarna.

2.1 Val av metod

Främst används kvantitativa metoder i kandidatuppsatsen för att få fram resultatet. Det vill säga insamling av ren fakta genom ett flertal tester. Metoden för att testa de inbyggda brandväggarna har valts genom studerande av vedertagna metoder, dessa har sin grund både i den litteratur vi använder i arbetet samt andra källor vi tar upp i följande kapitel.

2.1.1 Tester

För att svara på frågeställningen används två stycken olika tester, en Säkerhetstest (benämns sTest), som är rent kvantitativ. Samt ett funktionalitetstest (benämns fTest), som även den är kvantitativ.

2.1.1.2 Säkerhetstest

sTest berör den direkta tekniska säkerheten till skydd mot de hot som finns på Internet. De olika metoderna som använts har varit:

- Informationssökning via skanning
- Svaghetstest, både direkt attack och utnyttjande av resurs

2.1.1.3 Funktionalitetstest

En undersökning som SCB har genomfört under 2002 av privatpersoners Internetanvändning [27] användes för att kunna styrka fTest och de urval som har gjorts där.

2.1.2 Verktyg

De verktygen som använts har tagits fram genom noggrant sökande på Internet och relaterade sidor för hacking, säkerhet och forskning samt i relevant litteratur i ämnet [2], [5], [25]. Utifrån detta har en gallring gjorts och bedömningar på respektive verktyg, så att de som använts ämnar sig bäst för ändamålet, det vill säga att testa och kontrollera de inbyggda brandväggarnas säkerhet och agerande. Möjligheten att utnyttja så kallade onlineverktyg har ej heller utnyttjats, anledningen ligger i kontroller av verktyget, både sett ur styrning vid tester och validering av resultat.

2.1.3 Litteraturstudium

I den litteratur som vår information främst har inhämtats från har varit från så pass ny som möjligt då livstiden är relativt kort inom säkerhetsämnet. Litteratur som berör säkerhet och brandväggar och som är skrivna före år 2000 har inte sökts då informationen måste vara så aktuell som möjligt. Vidare har det varit litteratur som sträcker sig kring nätsäkerhet, operativsystem samt om brandväggar.

Maximum Security har agerat som ett mycket bra referensverk, både i sökandet efter ytterligare källor, som verktyg för testerna, samt bakgrundsfakta till uppsatsen [5]. I allmänt om brandväggar har Brandväggar 24sju bland annat använts [1]. Den främst litteraturen som hämtats om Microsoft Windows XPs Internet Connection Firewall (ICF) är publicerad av Microsoft [4]. Likaledes är även den informationen om Red Hats inbyggda brandvägg varit främst varit representerad av sin konstruktör. Dels från Red Hats webbsida [16], men även Bill McCartys bok Red Hat Linux Firewalls [2] har legat till grunden för majoriteten av bakgrundsfakta både till IPTables och de inbyggda brandväggarnas uppbyggnad. Annan litteratur som använts för att beskriva vissa bakgrunds fakta har varit Stallings två verk om operativsystem [6] samt lokala nätverk [7]. Även Security in Computing av författarna Pfleeger har varit en av de litterära källorna [3].

2.1.4 Internet

Internet är det absolut främsta verktyget som använts i informationssökningen, både till att, som nämnts, tagit fram verktygen och litteratursökande. Även annan information så som Requests for Comments (RFC) [9], [10], [11], [12], [13], [14], [15], manualer till verktygen och säkerhets- samt hackerwebsidor har legat till grund för detta arbete. Internet är i ständig rörelse och förändring och de länkar som relaterats till i källförteckningen är till de webbsidor där verktygen hämtats från och texternas absoluta ursprung då många texter och verktyg länkas vidare eller är tagna ur sitt sammanhang. Varje källa och verktyg som hämtats från Internet har noga granskats ur ett källkritiskt perspektiv och värderats var för sig.

2.1.5 Uppsatser och rapporter

Tidigare kandidatarbeten från Blekinge Tekniska Högskola (BTH), samt ett flertal publicerade vetenskapliga artiklar har undersökts inför detta arbete. Den främsta rapporten som använts har varit från det Amerikanska institutet för standard och teknologis (NIST) rekommendation för hur man skall testa och kontrollera sitt nätverk [25], detta har bland annat legat till grund för de metoderna som använts för testerna av de inbyggda brandväggarna.

Från BTH har ett par kandidatarbeten undersökts, där speciellt en om Datasäkerhet för hemdatorer var av särskilt intresse. Skriven av Elisabeth Olinder och Mari Pettersson, skrevs under 2001. De undersökte datasäkerheten ur hemmaanvändarens perspektiv, hotbilden vid Internet användning samt vilket skydd en personlig brandvägg kan erbjuda. Deras slutsats var att mycket av ansvaret på datasäkerheten ligger på användaren, samt att en brandvägg lätt kan vagga in en användare i falsk säkerhet [26].

2.2 Reliabilitet och Validitet

Verktygen i testerna har validerats genom noggrant testande, samt kontroll av den trafik de genererat mot de inbyggda brandväggarna. Paketsniffning genom tcpdump [22] eller windump [23] har gjorts för att kontrollera och säkerställa både resultat och verktygens utförande. Alla tester har genomförts i flera omgångar för att säkerställa resultatets reliabilitet.

3. TEORIBAKGRUND

Detta avsnitt kommer att rikta in sig främst på att ge en kortare beskrivning av de två operativsystemen, vad en brandvägg är och hur den definieras samt den tekniken som kommunikationen över Internet bygger på.

3.1 TCP/IP protokoll arkitekturen

Kommunikation kan delas upp i tre större delar: applikationer, datorer och nätverk. Exempel på applikationer är e-postprogram och webbläsare, dessa gör att två användare kan kommunicera med varandra. Datorerna är anslutna till nätverk och datan som överförs går från applikation till dator över nätverk vidare till mottagande dator och informationen (datan) visas genom någon form av applikation. För att strukturera upp detta i en modell, kan detta göras genom TCP/IP protokollarkitekturen som organiseras enligt fyra lager ([7] lade även in det fysiska lagret i denna struktur) [7], [2], [6].

Applikationslagret är som nämnts där olika program utnyttjar och visar den data som skickas eller tas emot. Program kan vara allt från Internet Explorer till ICQ. För att kommunikation med applikationer ska vara möjlig över ett nätverk behöver de bygga på TCP/IP arkitekturen. Transport- och Internetlagret har sin grund i TCP/IP familjen, samlingsnamnet för protokollen i dessa två lager [7], [2], [6].

Transportlagret förmedlar data mellan applikationslagret och Internetlagret. Lagret består av två protokoll, Transmission Control Protocol (TCP) [11] och User Datagram Protocol (UDP) [12]. Internetlagret fungerar som en tjänst som förmedlar paket. Denna tjänst används av de lager som ligger ovanför. Den kapslar in data i paket som kallas för datagram. Dessa förmedlas sedan med hjälp av IP-protokollet [10]. IP väntar inte på att mottagaren ska svara utan skickar sina paket ändå. Detta kan göras då kontrollen och handskakningen görs av TCP i transportlagret ovanför [6]. Nätverkslagret, innefattar MAC-adresser och ett nätverks struktur. MAC-adresser är hårdvaruadressen till nätverkskortet som används för kommunikation och kan endast nås av andra noder inom ett nätverk [7].

3.1.2 TCP/IP familjen

TCP/IP familjen refererar till ett flertal protokoll som ansvarar för metoder att kommunicera mellan system och nätverk. Tjänster som bygger på TCP/IP familjens grund är bland annat [5]:

- Skickandet av e-post
- Fil överföring / nedladdning
- IM
- tillgång till World Wide Web (WWW)

3.1.2.1 IP

Internet Protocol (IP) är det vanligaste protokollet som sköter kommunikationen över Internet. IP anger den adress som datorn har på Internet eller inom nätverket. Allt från servrar, routrar till skrivare och PC kan ha en eller flera IP-adresser. Den behövs för att paketen skall hitta fram till rätt adress och kunna svara till rätt avsändare [10]. Det är det så kallade huvudet i IP-paketet som bär den viktiga informationen som gör att paketet skall hitta fram till rätt mottagare. Här ligger exempelvis information om avsändare, mottagare och om paketet är fragmenterat eller ej. Fragmentering innebär att man delar upp paketet i mindre delar, detta används dels när man skickar paket över olika typer av nätverk men kan även utnyttjas i försök att penetrera brandväggar [7]. Begreppet ’spoof’ syftar på att förfalska en IP-adress. Detta för att antingen försvåra bindandet till olagliga skanningar, eller för att helt enkelt utgöra sig för att vara någon annan i ett nätverk [3], [5].

3.1.2.2 TCP

Transport Control Protocol (TCP) är det protokollet som kontrollerar att datan kommer fram i rätt ordning och till rätt port hos mottagaren. TCP handhar de flaggor som används för att markera handskakning och hur kommunikationen skall skötas [11]. Det finns sex flaggor som ingår i TCP för att styra kontrollen av trafiken:

SYN - synkroniserar sekvensnumren under kommunikationens initiering.
ACK - bekräftelse på tidigare anrop.
FIN - meddelar att avsändaren inte har mer data att skicka.
URG - meddelar att paketet innehåller brådskande data.
PSH - används i kombination med windows i TCP huvudet för att få fram data.
RST - avslutar förbindelsen direkt.

Vid initiering av kommunikation används en så kallad trevägshandskakning. Den går till så att ett TCP-paket skickas från avsändaren med en SYN-flagga markerad. Mottagaren svara med en ACK samt en SYN i samma paket tillbaka. Efter detta svarar avsändaren med en ACK, och kommunikationen kan påbörjas. Hade exempelvis mottagaren inte accepterat kommunikationen hade datorn svarat med RST flaggan aktiverad i TCP-paketet. Den hade då avslutats. Sekvensnumret håller reda på TCP-paketet och i vilken ordning datan skickas [11].

Tabell 1.
Exempel trevägshandskakning:

Avsändare	Mottagare	Protokoll + flaggor
ALPHA	BETA	TCP : SYN
BETA	ALPHA	TCP : ACK + SYN
ALPHA	BETA	TCP : ACK

Vid exempelvis skanning manipulerar man oftast TCP-paketets flaggor för att lura en brandvägg. Vanliga manipulationer är NULL-flaggat TCP-paket, där man skapar paket som inte har några flaggor alls. Detta är ett paket som ej finns specificerat i [11], och benämns som ett anomalipaket. Andra exempel på vanliga anomalier är X-mas där URG,PSH och FIN eller alla flaggorna är aktiverade. För att kunna utnyttja detta i en skanning, skickar man så exempelvis ett X-mas-flaggat paket mot en mottagare med brandvägg. Vissa brandväggar kommer så på detta att svara med ett RST-flaggat TCP-paket där portarna är stängda, men inte svara alls där den har öppna portar, allt enligt RFC standard [11].

Tabell 2.
Exempel skanning med X-mas paket:

Avsändare	Mottagare:port	Protokoll + flaggor
BETA -->	ALPHA:20	TCP : URG+PSH+FIN
ALPHA -->	BETA:4210	TCP : RST
BETA -->	ALPHA:21	TCP : URG+PSH+FIN
BETA -->	ALPHA:22	TCP : URG+PSH+FIN
ALPHA -->	BETA:4210	TCP : RST
osv...		

Skanningen kommer här visa att ALPHA bland annat har port 21 öppen, då dess brandvägg inte svarade med en RST-flagga som den gjorde när porten var stängd. Förutom NULL och X-mas skanningar finns ett par andra manipulationer av TCP-paketets flaggor, dels 'stealth SYN' men även 'stealth FIN'. 'stealth SYN' skanning genomförs så att man skickar ett SYN-flaggat paket som liknar en initiering av en kommunikation, om mottagaren svarar med en SYN+ACK är porten öppen, om inte, svarar mottagaren med ett RST-flaggat TCP-paket. 'stealth FIN' agerar likt de andra två anomali skanningarna, förutom att det i detta fallet endast FIN-flaggan är aktiverad i TCP-paketet [11], [20].

3.1.2.2 UDP

User Diagram Protocol, eller Unreliable Diagram Protocol som det även benämns i vissa sammanhang är TCPs motsvarighet på transportlagret. Skillnaden är att UDP inte ansvarar för att paketen kommer fram utan guidar bara paketen till rätt port. Den använder sig således inte av flaggor likt TCP gör [12].

3.1.2.3 ICMP

Internet Control Message Protocol (ICMP), är ett kontrollprotokoll som inte bär någon applikationsdata utan endast information om nätverket, bland annat vilka datorer som kan nås. Exempel på verktyg som bygger på ICMP är '*ping*'. Det ping gör via ICMP är att den skickar ut en så kallad '*echo - request*' för att se om den avsedda datorn svarar på tillropet. Om den är inställd på att svara på ICMP anrop skickas ett '*echo - reply*' till svar att den är vid liv. Annars svarar närmsta router med ett '*echo – host unreachable*' [8].

3.2 Brandväggar

3.2.1 Historik

Idén om hur brandväggar kan fungera har funnits med länge. Det började med 'reference monitor'. En referece monitor agerar som en mur runt ett operativsystem eller mjukvara som man vet att man kan lita på. Detta uppnåddes genom att samla all kontroll för accesser för exempelvis filer, minne och så vidare, på ett och samma ställe. På detta sätt hade man kontroll över alla accesser som utfördes på datorn [3].

Den första officiella brandväggen använde sig av diverse filtreringsregler, och var ganska begränsade, och det uppstod ofta problem med att få filtreringsreglerna rätt [1]. 1993 släpptes FWTK (Firewall Tool Kit) till allmänheten av Trusted Information Systems (TIS) [14]. Meningen med FWTK var bland annat att tillhandahålla en mängd verktyg för att kunna bygga brandväggar, samt att öka säkerheten för Internetanvändarna [1], [13]. Kort efter detta släpptes en brandvägg av företaget CheckPoint, som kom att kallas för Firewall-1 [15].

3.2.2 Funktion och syfte

Varför ska man ha en brandvägg? En brandvägg är ett första skydd för en dator eller ett nätverk mot otillåtna angrepp och resursutnyttjande. En brandvägg kan också konfigureras så att man begränsar vad en användare inom ett nät får utnyttja för tjänster. En brandvägg fungerar ungefär som en vägg som reglerar vilken trafik som får passera in och ut genom ett nät eller dator. Trafiken passerar genom en mängd portar som kontrolleras av brandväggen. Som standardvärde har många tjänster fördefinierade portnummer, exempelvis så har ftp-protokollet port 20 och 21 [9].

3.2.2.1 Brandväggslösningar

När man talar om brandväggar finns det en mängd olika lösningar att titta på. Nedan följer ett par olika lösningar av brandväggar som tas upp i ett flertal olika litteraturstudium [3], [5], [1].

- Paket-filtrering
- Stateful Inspection
- Personlig brandvägg

Paket-filtrering bearbetar varje paket för sig och beslutar för varje paket om de ska accepteras eller inte. Man kan med detta besluta att tillåta eller stoppa specifika portar eller IP-adresser. Problemet med paket-filtrering är dock att den är stateless, det vill säga att den enbart kontrollerar portar och/eller IP-adresser. En så kallad 'Stateful Inspection' är en stateful brandvägg som granskar hela paketen mer ingående och följer dess väg och håller koll på om de är en del i en större kommunikationsdel, en session.

En personlig brandvägg är en mjukvara som körs från en och samma dator där användaren sitter. Exempel på där personliga brandväggar kan användas kan vara hos användare eller småföretagare och mindre nätverk.

3.2.3 Hot på Internet

Alla har vi hört ord som cracker, hacker och så vidare. Men vad betyder orden egentligen, och på vilket sätt kan de påverka en dator exempelvis ute på Internet? När datorer precis hade kommit var ordet hacker vanligt. Den vanliga uppfattningen då var att en hacker var en person som hade en stor insikt över hur datorer fungerade. Detta har nu utvecklats till att syfta på en person som utför kriminella handlingar. De hackers som inte haft avsikten att förstöra för någon annan gillade inte att få den stämpeln på sig utan gav de hackers med onda avsikter namnet crackers [1], [3].

Den vanligaste typen av attacker som utförs mot en dator görs av så kallade script kids. Som namnet antyder är de ofta unga och har ingen riktigt kunskap inom cracking utan använder redan färdiga verktyg eller scripts som de hittat ute på Internet [3], [5]. En annan grupp kallas för Black Hats. Denna grupp består oftast av personer med mycket god kunskap inom programmering, kunskap inom nätsäkerhet eller liknande. Till skillnad från script kids så planerar de sina mål noga och har oftast en speciell orsak att attackera just där [5]. White Hats är en annan grupp vars medlemmar oftast har sin grund i Black Hats. Många av dessa arbetar

för andra företag för att undersöka eller testa deras säkerhetssystem. Medlemmarna i White Hats har inga onda avsikter med sina intrångsförsök, utan är bara ute efter kunskap eller liknande om systemet [5].

Trojaner, virus och maskar är tre andra större hot ute på nätet, hot som användaren själv är den utlösande faktorn till. Virus och maskar har som uppgift att förstöra och sprida sig vidare på Internet [3]. Ett sista hot, som dock inte drabbar en vanlig användare allt för ofta är DoS attacker, men de kan även utsättas för att vara upphov till dessa destruktiva attacker, precis som i trojan, virus och mask spridandet kan en användares dator infekteras och utnyttjas i användandet av DoS attacker [5]. DoS står för Denial of Service och är en av de senare årens vanligaste attacker mot servrar och enskilda datorer. Attacken syftar till att slå ut datorn och dess möjlighet att kommunicera över Internet genom att överbelasta den med extremt många anrop. Metoderna för denna typ av attack är många och har en bred skala av effektivitet [3].

3.3 Windows XP och Red Hat Linux

De två operativsystemen valdes, dels för sina inbyggda brandväggar och dels för att kunna jämföra Windows nyaste operativsystem med ett Linux system.

3.3.1 Microsoft Windows XP

Windows XP Professional Edition släpptes hösten 2001 av Microsoft och har sedan dess tagit allt större marknadsandelar av operativsystemen på marknaden där Microsoft har hela 95 % av marknaden [17]. Windows XP är utvecklat för att vara ett betydligt säkrare system och mer stabilt än sina föregångare från Microsoft [18].

3.3.2 Red Hat Linux

Red Hat Linux 8.0 med kernel version 2.4.18 släpptes hösten 2002 [16], här har användarvänligheten förbättrats och det grafiska gränssnittet utvecklats i kampen mot Microsoft. Linux samlade operativsystem har idag under 1 % av den totala PC marknaden [17] där Red Hat är en av de främsta Linux versionerna vad gäller marknadsandelar.

3.3.2.1 IPTables

IPTables är en brandväggsapplikation som konfigureras via kommandoprompten och har sedan Red Hat Linux 7.0 haft IPTables inkluderat i operativsystemet. Fördelen med IPTables mot tidigare Linux brandväggsapplikationer är att IPTables använder sig av stateful paket filtrering, vilket innebär att den kan blockera inkommande paket som inte är relaterade till en redan etablerad kommunikation. IPTables kan konfigureras så den blockerar eller tillåter trafik på specifika portar eller mot givna IP-adresser eller nätverk. Den är även konfigurerbar efter specifika protokoll så som TCP, UDP och ICMP samt finns en möjlighet att anpassa den efter specifika TCP-flaggor, där man kan bestämma vilka olika former och kombinationer som skall godkännas för kommunikation. Slutligen kan även IPTables konfigureras så att den genererar loggning på trafik mot datorn [2].

4. Undersökning

I följande kapitel kommer det att tas upp hur undersökningen genomförts rent tekniskt, strukturen på nätverket, operativsystemen och de olika verktygen som använts. Här kommer det kommer även att beskrivas de olika teknikerna vad gäller testerna och hur de genomförts. De två brandväggarna kommer även att beröras ur ett tekniskt perspektiv.

Följande benämningar gäller för denna undersökning. En dator som är själva försöksobjektet med respektive operativsystem och inbyggd brandvägg, benämns: ALPHA. För att specificera än mer har vi benämnt Red Hat Linux 8.0 installationen som L-ALPHA och Windows XP installationen som W-ALPHA. En dator där intrångsförsök och andra tester kommer att utföras ifrån BETA.

4.1 Installation av operativsystem och verktyg

4.1.1 ALPHA

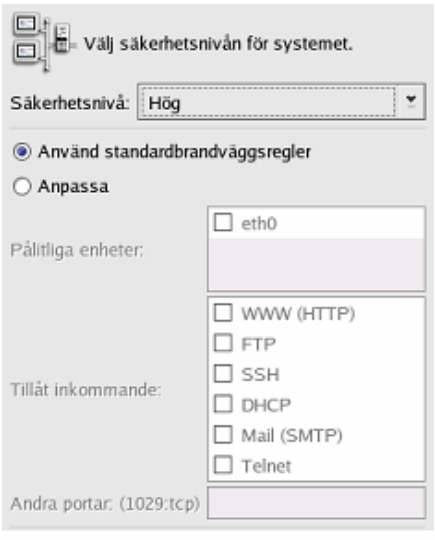
På denna dator installerades två operativsystem för att använda oss av exakt samma prestanda vad gäller hårdvaran. Även de två operativsystemen som installerades hade så pass likartade inställningar som möjligt.

Hårdvara:
Processor *Pentium II Celeron 500 Mhz*
RAM *128 MB*
Hårddisk *1.98 G för XP / 1.98 G för Red Hat*
Nätverkskort *10/100 Mbit*

4.1.1.1 L-ALPHA

Operativsystem: *Red Hat Linux 8.0 Workstation installation.*
Brandvägg: *Security Level Configuration Tool (SLCT)*
Skydd: *Högsta möjliga.*

Vid installationen av operativsystemet får man vid konfigurationen av uppkoppling valmöjligheten att använda sig av Red Hats inbyggda brandvägg – Security Level Configuration Tool (förkortas hädan efter SLCT). Säkerhetsnivån som valdes var ’Hög säkerhet’. Övriga valmöjligheter var ’Mellan’ och ’Ingen brandvägg’. Dessa nivåer har alla fördefinierat vilka portar och tjänster som skall tillåtas. Men man kan även konfigurera den själv genom att tala om vilka portar som ska vara öppna. Detta val innebär att den inbyggda brandväggen tillåter DHCP samt DNS svar enligt konfigurations



figur 1. SLCTs konfigurations inställningar.

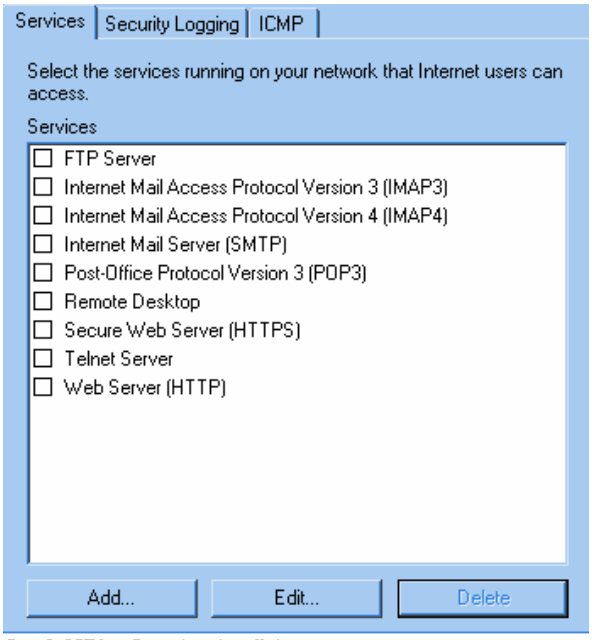
texten. Installationstexten förklarar: *'Hög säkerhet: Hög säkerhet kommer ditt system inte att acceptera anslutningar som inte uttryckligen har angivits av dig. Som standard tillåts endast följande anslutningar: DNS svar och DHCP.'* Efter själva installationen kunde SLCT hittas under 'Main >> Annat >> Säkerhetsinställningar' från skrivbordet i Red Hat Linux. Samma typ av konfigurations valmöjligheter finns här som under installationen.

SLCT gör så att den förenklar användandet av IPTables som ligger till grund för den inbyggda brandväggen. Den kan ses som ett grafiskt och mycket förenklat verktyg för konfiguration av IPTables, med medföljande restriktioner som nämnts ovan.

4.1.1.2 W-ALPHA

Operativsystem: *Microsoft Windows XP Professional*
Brandvägg: *Internet Connection Firewall (ICF)*
Skydd: *Högsta möjliga.*

Installationen av ICF sker utan användarens vetskap vid installation av operativsystemet, om inte användaren väljer att installera sina nätverksdrivrutiner, då sker installationen och uppstarten av ICF automatiskt. Inga förval på säkerhets nivå eller tillåtande av tjänst har man som valmöjlighet. Om man däremot senare väljer att installera ICF, sker detta genom att kryssa i en så kallad checkbox ruta.



figur 2. ICF konfigurations inställningar.

Konfigurations möjligheter som finns är att man kan tillåta vissa tjänster genom att öppna portar för detta, samt sköta loggning av den inkommande trafiken som ansluter mot datorn och dess ICF [19], [4]. Konfigureringen till ICF hittas under 'Start >> Settings >> Network Connections >> LAN Status >> Properties >> Advanced >> Settings'.

Metoden ICF använder för att kontrollera trafiken kallas 'table method'. Med denna metod menas att den håller reda på en lista av utgående och inkommande IP-adresser.

Om exempelvis användaren i sin webbläsare gör en förfrågan efter www.aftonbladet.se läggs dess IP och session in i utgående tabell, när(om) svaret anländer accepteras detta först efter en kontroll mot utgående tabell. Finns inte IP-adressen i tabellen förnekas den inkommande trafiken helt. ICF arbetar mot sin tabell och inte på protokoll basis. Med detta menas att så länge det är användaren som gör förfrågan så kommer trafiken att passera ICF friktionsfritt. Den är stateful [4]. Medvetna brister i ICF som Microsoft upplyser om är att den inte skyddar mot virus och maskar, ej heller om en trojan ligger på datorn. På grund av att ICF inte kontrollerar trafik som går ut, utan endast lägger dem till sin tabell [4], [19].

4.1.2 BETA

På BETA användes operativsystemet Red Hat Linux 8.0 med Workstation som installation. Här installerades de verktyg som användes och kontrollerades inför testerna.

4.1.3 Verktyg

De verktyg som använts i brandväggstesterna sTest och fTest är följande :

- Ping
- Nmap 3.20
- Nessus 2.0
- Netcat 1.10
- Tcpdump/Windump

Dessa verktyg har valts i sina senaste möjliga uppdateringar och stabila versioner samt utifrån de operativsystem vi testade.

Ping: Använder sig av ICMP för att bland annat lokalisera datorer. Det man gör är att skicka en echo request med hjälp av ICMP för att ta reda på om en dator svarar och är aktiv. Ping applikationen finns både i Windows XP och Red Hat Linux 8.0 och behöver inte installeras separat.

Nmap version 3.20: Nmap är ett skanning verktyg, främst för att kartlägga hela nätverk, men fungerar minst lika bra för att söka på specifika datorer i ett nätverk. Det finns ett flertal så kallade växlar för att använda nmaps alla olika möjligheter. Dessa bestämmer de villkor den ska följa i sin skanning av en dator. Nmaps olika egenskaper är att att skicka manipulerade paket med fördefinerade flaggor, falsk avsändaradress, operativsystems identifiering, anomaliska paket, stealth skanning, med mera. Dess syfte är främst att se vilka tjänster en dator besitter, det vill säga vilka portar som är synliga utåt sett, eller bara att ta reda på vilket operativsystem som ligger på datorn [20].

Nessus, version 2.0.1: Nessus bygger på verktyget nmap, och skannar även den av datorn efter öppna portar. Vad den vidare gör är att kontrollera och testar om denna öppna port tillhandahåller en tjänst som har ett känt säkerhetshål eller problem. Nessus försöker sig på intrångsförsök som den dels konstant kan uppdateras med, både vad gäller kända säkerhetshål och svagheter, samt med nya applikationer som kan knytas till Nessusskanningen. Dessa kallas gemensamt för ’plugins’. Exempel på detta kan vara nmap, men också andra skannings- och så kallade ’brute force’ applikationer. Nessus bygger på en serverprogramvara som skanningen utgår ifrån samt en klient som styr denna skanning, vilka val och inställningar som gäller [21].

Boken Red Hat Linux Firewalls [2] utfärdare en varnar för att Nessus kan generera felaktiga rapporter. Detta på grund av att Red Hat menar att de själva genomför uppdateringar av felaktiga applikationer som bär på säkerhets risker, något som då Nessus i vissa fall kan ignorera och ändå generera en rapport om. Samtidigt menar dock författaren att Nessus är ett av de absolut bästa verktygen för att kontrollera en brandväggs effektivitet.

Tcpdump / Windump: Ett verktyg för att logga inkommande och utgående trafik. Det finns både för Windows och Linux. För att validera testerna har vi använt oss av verktyget Tcpdump[22] för L-ALPHA och Windump[23] för W-ALPHA.

Netcat 1.10: Ett gammalt verktyg från 1996, som trots detta är mycket effektivt för tester av system. Netcat kan bland annat användas både som en trojan för att ge tillgång till ett operativsystem eller för skanning av portar [24]. I säkerhetstestet användes en Netcat applikation på BETA och en på ALPHA för att skapa en kommunikation mellan de två datorerna.

4.2 Testerna

Inför varje test har brandväggarna validerats att de varit igång för att skapa rättvisande resultat utifrån de förutsättningarna testerna utförts. ICF har kontrollerats genom en ren visuell kontroll, samt att inga extra portar i jämförelse med grundinställningarna var öppna. SLCTs regler kontrollerades genom kommandot 'iptables -L' [aa], [ab].

4.2.1 Säkerhetstest

sTest har genomförts enligt följande schema:

- skanning, verktyg Nmap 3.20
- vulnerability skanning, verktyg Nessus 2.0
- idle skanning test, verktyg Nmap 3.20
- Utgående trafik, verktyg netcat 1.10

Som underlag för diskussionen har resultatet från dessa tester tagits fram, samt loggar från W-ALPHAs inbyggda brandvägg och Tcpdump/Windump.

4.2.1.1 Skanning

Grundläggande informationssökning genom nmap och ping. Här vill vi visa hur mycket information man kan utvinna ur ALPHA och se vad den inbyggda brandväggen skyddar mot för olika former av skanningsförsök. Den primära informationen som sökts har varit om den är vid liv, portar som operativsystemet lämnat öppna, samt vilket operativsystem som ligger på ALPHA, en så kallad operativsystems-identifiering.

4.2.1.2 Vulnerability skanning

För att testa brandväggen på ALPHA har verktyget Nessus använts, som med hundratals plugins testar kända svagheter och om de svagheterna är synliga när brandväggen är på. Testet utfördes också utan brandvägg för att kontrollera Nessus effektivitet, men också för att se vad och hur mycket den egentligen skyddade ALPHA. Nessusskanningen kördes mot alla TCP och UDP portar med samtliga plugins på.

4.2.1.3 Idle skanning test

I detta test kontrollerades om ALPHA kunde användas som mellanhand i exempelvis skanning av annan dator. Detta är dels ett problem som operativsystemet står inför, men som även den inbyggda brandväggen kan skydda mot om denna svaghet finns. Idle skanning genomförs genom att skanna en utvald dator och ange ALPHA i nmap som mellanhand. Den utvalda datorn gör så att den skickar svaren på skanningen till den som den tror har gjort skanningen, nämligen ALPHA. Detta sker samtidigt som BETA kontrollerar de svaren ALPHA får, genom att se till datorns sekvensnummer på port 80, som därefter används som räknare [20].

4.2.1.4 Utgående trafik

Det verktyget som använts på båda operativsystemen har varit Netcat[24] som legat under de mer frekventa och använda portarna för DNS, DHCP samt högre icke tjänsteportar. Testet har genomförts för att kontrollera hur de inbyggda brandväggarna agerar mot utgående trafik, samt latent lyssnande applikationer bakom de inbyggda brandväggarna. I och med att litteraturen från Microsoft [19], [4],och även när man kontrollerar reglerna för IPTables[aa], har vi redan i förarbetet upptäckt att ingen av de inbyggda brandväggarna kontrollerar utgående trafik.

4.2.2 Funktionalitetstest

Utgångspunkten har här varit SCBs undersökning om svenska folkets Internetvanor, vilka former de använder Internet till under 2002 [27]. 3092 personer i åldern 16-74 år svarade på olika frågor om sina Internet vanor. Den fråga vi har tagit del av och utnyttjat i denna uppsats löd: ”*För vilket eller vilka av följande privata syften har Du använt Internet under tiden januari t.o.m. mars*”. De förfrågade fick välja ur 20 olika typer av tjänster, allt från spel till ren surfning. Därefter delade SCB in svaren i fyra olika grupperingar. Kommunikation, Informationssökning, myndighetskontakter och Köp & Försäljning. Kommunikation innefattade skicka och ta emot e-post, chatta och IM. Informationssökning har SCB bland annat räknat in att söka information om varor och tjänster, distansutbildning, ladda ner musik och spela spel. Myndighetskontakter innefattade att ladda ner blanketter eller allmän informationssökning från myndighetssidor och slutligen köp och försäljning på Internet. Fördelningen blev då enligt följande:

Kommunikation 58,5 %
Informationssökning 67,4 %
Köp och försäljning 47,4 %
Myndighetskontakt 42,0 %

Det vi gjort är att ha sökt upp applikationer för respektive delgrupp och testat funktionaliteten i kombination med den inbyggda brandväggen. Urvalet på applikationer har varit att först och främst valt de applikationer som ligger förinstallerade på operativsystemet, annars har vi tagit en väl fungerande och testad applikation för det ändamålet, det är dock viktigt att lyfta fram att det främst är tjänsterna och inte de specifika applikationerna som ska testas.

Under kommunikationstjänster har följande applikationer valts. För beskrivning av dessa applikationer så finns detta under Appendix A [af], [ag]. För Windows XP; ICQ, Windows Messenger, Outlook, IMP och mIRC. Och för Red Hat Linux; LICQ, Gaim, Ximian, IMP och

X-Chat. För Informationssökning fick de bägge operativsystemen tre stycken applikationer var. Ett för informationssökning via webbsidor, en för att ladda hem information med hjälp av FTP och slutligen en applikation för att behandla nyhetsgrupper. För Windows XP; Internet Explorer, Cute FTP Pro och Outlook (nyhetsgrupper). För Red Hat Linux; Mozilla, gFTP och Knode. Köp & Försäljning gick till på samma sätt för båda operativsystemen. För att tillgodose dessa tjänster användes Internet Explorer användes till Windows Xp och till Red Hat, Mozilla. Detta likaså till Köp och försäljning.

Testerna har genomförts med allt från en till ett flertal repetitioner beroende på vilket test och applikation som kördes per brandväggskonfiguration. Vid misslyckat försök har vi stängt av den inbyggda brandväggen och gjort nya försök för att se om den är orsaken till felet, samt kontrollerat tcpdump/windump rapporterna. I fTest har vi valt att även anpassa testerna efter vilka operativsystem som låg på datorn. Exempelvis har vi gjort valet att inte göra speltester på Red Hat Linux 8.0 då inga kommersiella spel används eller finns till detta operativsystem. Dessa tester utfördes både mot BETA, men likaväl andra datorer ute på Internet beroende på vilken form av applikation och tjänst vi testade.

5. RESULTAT

I detta kapitel presenteras de resultat som testerna har genererat. En total sammanställning samt den oformaterade informationen från de olika testerna ligger i Appendix A.

5.1 Resultat Säkerhetstest

5.1.1 Informations sökning

Vid kontroll av ALPHA visade dessa portar vara öppna för inkommande tjänsteutnyttjande bakom respektive inbyggd brandvägg.

Tabell 3 [c], [d]

Protokoll	W-ALPHA	L-ALPHA
TCP	135,139,445,1025,1027,5000	22,111,1024,6000
UDP	123,135,137,138,445,500,1900,2234	111,1024

Första testet som genomfördes mot ALPHA var ’ping’ för att se om den var synlig utåt. Här svarade L-ALPHA, men däremot inte W-ALPHA på ICMP-anropet. I de övriga testerna fortsatte W-ALPHA att vägra svara på alla olika former av skanningar som vi utförde. Det ICF gjorde var att förvägra alla skanningar och anrop som den själv ej initierat. Detta gällde också i anomalitestet, fragmenterade och UDP skanningen.

Operativsystems-identifiering (OS-id) som genomfördes med hjälp av nmap mot L-ALPHA genererade en gissning på att operativsystemet var Linux med en Kernel mellan 2.4.0 och 2.5.20 i och med att den inte hittade några öppna portar i skanningen, annars hade gissningen varit mer exakt. Följande scenario visades i tcpdumpen från BETA i OS-id testet:

Tabell 4 [j]

Avsändare	Mottagare	Protokoll+flaggor
BETA >	L-ALPHA	TCP:SYN
L-ALPHA >	BETA	ICMP - TCP port unreachable
BETA >	L-ALPHA	TCP:ACK
L-ALPHA >	BETA	TCP:RST
BETA >	L-ALPHA	TCP:FIN,PSH,URG
L-ALPHA >	BETA	TCP:RST+ACK
BETA >	L-ALPHA	UDP
L-ALPHA >	BETA	ICMP - UDP port unreachable

Både trevägshandskakningen och stealth SYN förvägrades av de två operativsystemens inbyggda brandväggar och gav inget gensvar. Däremot anomalierna visade på skillnader på ALPHAs olika inbyggda brandväggar. W-ALPHA förvägrade som nämnts åter alla inkommande paket från skanningen medan L-ALPHA svarade med RST+ACK i skanningen mot stängda portar, och inte alls mot öppna. Både FIN, X-mas och NULL skanningen gav följande resultat mot L-ALPHA:

Tabell 5 [r] X-mas skanning genom nmap:

Port	Tillstånd	Tjänst
22/tcp	open	ssh
111/tcp	open	sunrpc
1024/tcp	open	kdm
6000/tcp	open	X11

Nedan återfinns W-ALPHAs agerande mot accepterad trafik samt skanningen:

Tabell 6 [ac]

Exempel uppstart av Internet kommunikation, ICFs loggning:

Agerande	Protokoll	Avsändare	Mottagare : port	Flaggor
OPEN	UDP	ALPHA	194.47.139.1 : 1900	-
OPEN	UDP	ALPHA	194.47.129.10 : 53	-

Exempel nedkoppling av Internet kommunikation ICFs loggning:

Agerande	Protokoll	Avsändare	Mottagare : port	Flaggor
CLOSE	UDP	ALPHA	194.47.139.1 : 1900	-
CLOSE	UDP	ALPHA	194.47.129.10 : 53	-

En förvägran – 'DROP'- från ICF, detta skedde under alla skanningar vi genomförde:

Agerande	Protokoll	Avsändare	Mottagare : port	Flaggor
DROP	TCP	BETA	ALPHA : 5000	FIN+URG+PSH
DROP	TCP	BETA	ALPHA : 1024	FIN+URG+PSH

Spoofad adresser gav inte någon skillnad på nmap resultaten, ej heller fragmenterade paket lyckades penetrera de inbyggda brandväggarna. I SLCTs regler låg DNS-servern för ALPHA som accepterad trafik [aa]. Genom nmap förfalskades denna adress i skanningen samt avsändar port för att likna DNS-servern, dock kunde inte skanningsverktyget generera något gediget resultat. Tcpdump visade dock att SLCT accepterade denna trafik trots att den var förfalskad som visas i tabell 7.

Tabell 7 [D]

Avsändare	Mottagare	Protokoll : port
Spoofad DNS-server	ALPHA	UDP : 111
Spoofad DNS-server	ALPHA	UDP :112
ALPHA	DNS-server	ICMP 'UDP port 112 unreachable'

5.1.2 Svaghetstest

För att se om idle-skanningen skulle ge resultat genomfördes testet mot ALPHA med den inbyggda brandväggen avstängd. Red Hats operativsystem medför att det inte är möjligt att genomföra idle skanning, i och med att de använder slumpmässiga sekvensnummer, medan Windows XP inte gör det. På detta sätt kunde vi skanna andra datorer med W-ALPHA som mellanhand. Med ICF på skyddades dock W-ALPHA från detta genom att förvägra alla mellanstegspaket och gjorde detta resursutnyttjande omöjligt.

Nessus skanningen, genererade ett par säkerhetsvarningar för L-ALPHA och W-ALPHA. De varningarna som utfärdades mot W-ALPHA kunde avfärdas då port 80 som Nessus varnade för var stängd och inte erbjöd någon webbserver tjänst. Skanningen mot L-ALPHA innehöll även den ingen ny information som vi tidigare ej funnit genom nmaps skanningar. Nessus presenterade sju säkerhetsnoteringar och en varning, detta innebar ingen skillnad om inbyggda brandväggen var på eller ej.

Netcat användes ur det syftet att bland annat kontrollera hur ICF och SLCT reagerade på tjänster som låg och lyssnade på öppna portar i de inbyggda brandväggarna. Testerna genomfördes i tre steg; utan brandvägg, bakom portar som var öppna utåt mot annan tjänst och när den inbyggda brandväggen först var avstängd då uppkopplingen skedde och därefter startades när kommunikationen påbörjats. När den inbyggda brandväggen inte var påslagen var det inga problem att skriva och läsa data mellan ALPHA och BETA. I testet där Netcat

låg och lyssnade på samma port som annan tjänst så fångades även denna kommunikation upp av respektive inbyggd brandvägg.

I tredje Netcat testet, när vi hade etablerat kontakt mellan avsändare och mottagare, startades den inbyggda brandväggen för att se om den avbröt kommunikationen. ICF gav ingen pardon och klippte av kommunikationen omedelbart, däremot SLCT tillät fortsatt full access att skriva och läsa data till L-ALPHA [B]. All kommunikation gjordes omöjlig när brandväggarna var igång på ALPHA och initiering av kommunikation försökte påbörjas.

5.2 Resultat Funktionalitetstest

Det första funktionalitetstest som gjordes bestod utav två stycken Instant Messengerprogram. Windows Messenger för W-ALPHA och Gaim för L-ALPHA. Gaim använder sig av AOLs (America Online) servrar och konton för att kommunicera. Dessa tester lyckades utan några problem med brandväggen påslagen. Värt att nämna är att varken ’skicka fil’ eller ’ta emot fil’ fanns tillgängliga för test i Gaim.

Tabell 8 [H], [I]

Windows Messenger/Gaim	W-ALPHA	L-ALPHA
Skicka meddelande	lyckat	lyckat
Skicka fil	lyckat	finns ej
Ta emot fil	lyckat	finns ej
Chat	lyckat	lyckat

Testningen fortsatte med ytterligare ytterligare två Instant Messengerprogram. ICQ för W-ALPHA och LICQ för L-ALPHA. Som resultatet visar misslyckades ’ta emot fil’ för både W-ALPHA och L-ALPHA. Misslyckades gjorde även ’Chat’ för W-ALPHA. I LICQ fanns det ingen ’Chat’ funktionen att testa.

Tabell 9 [F], [G]

ICQ/LICQ	W-ALPHA	L-ALPHA
Skicka meddelande	lyckat	lyckat
Skicka fil	lyckat	lyckat
Ta emot fil	misslyckat	misslyckat
Chat	misslyckat	finns ej

För e-posttesterna användes Microsoft Outlook för Windows XP och för Red Hat Linux 8.0 användes ett program som hette Ximian. Testningen gick till så att e-postprogrammen fick skicka samt ta emot e-post, samtidigt som TCPdump respektive Windump mätte trafiken beroende på om det var W-ALPHA eller L-ALPHA som kördes. Testet av nyhetsgrupper kördes på W-ALPHA genom Outlook då det fanns en funktion inbyggd i denna applikation som gjorde detta möjligt. På L-ALPHA gjordes testet med hjälp av programmet KNode. För både L-ALPHA och W-ALPHA användes nyhetsservern news.grc.com. Webmailtestet utfördes genom Blekinge Tekniska Högskolas online e-postprogram. Även där gjordes testerna ’skicka/ta emot e-post’.

Tabell 10 [J], [K]

Outlook/Ximian	W-ALPHA	L-ALPHA
Skicka e-post	lyckat	lyckat
Ta emot e-post	lyckat	lyckat

IRCtestet gjordes genom att koppla upp W-ALPHA och L-ALPHA mot en specifik server.
I detta fallet användes efnet.demon.co.uk. På W-ALPHA använde vi oss av mIRC och på L-ALPHA X-Chat. Vid sökningstestet så användes en vanlig sökmotor. I detta fallet blev det

Google (http://www.google.com). Varken W-ALPHA eller L-ALPHA hade några svårigheter att genomföra dessa tester med brandväggarna på.

Mediaspelare för W-ALPHA var Real One. L-ALPHA körde Real Audio 8. Testet bestod i att ’streama’ en musikvideo från www.svt.ses hemsida. FTPapplikation för W-ALPHA var CuteFTP och för L-ALPHA Gftp, dessa tester bestod endast av nedladdning. Formulärnedladdning och läsning skedde med Internet Explorer. för W-ALPHA, samt Mozilla för L-ALPHA. Under Köp & Sälj användes Internetbanken SEB för båda operativsystemen och beställning av vara gjordes från www.sf.se där köpet fullbordades.
Formulär nedladdningen och läsningen sker på samma vis som en vanlig nedladdning, antingen över port 80 eller 443 (https).

Det spel som testades till W-ALPHA var Warcraft III. Spelet testades på så vis att först så startade W-ALPHA en multiplayer session som server, varpå en annan dator försökte logga in som klient. Testet utfördes först med brandväggen påslagen och då misslyckades inloggningen av klienten. När den inbyggda brandväggen var avslagen fungerade multiplayer sessionen utmärkt. Nästa test bestod i att W-ALPHA, med den inbyggda brandväggen påslagen, försökte att logga in som klient på en annan dator som agerade server. Detta lyckades med ICF igång.

Tabell 11 [R]

Spel	W-ALPHA	L-ALPHA
Klient	lyckat	finns ej
Server	misslyckades	finns ej

6. DISKUSSION

I detta avsnitt svarar vi på vår frågeställning genom att diskutera resultatet.

Hur klarar den inbyggda brandväggen av de vanligaste Internettjänsterna som användarna utnyttjar? I undersökningen kring funktionalitet visade det sig att det lika mycket berodde på hur applikationen agerade som på den inbyggda brandväggen att de fungerade i symbios. Så länge som det var användaren som initierade kommunikationen fungerade trafiken i alla former av kommunikation. Så i stort sett all form av tjänsteutnyttjande klarade funktionalitetstestet. Både Red Hat Linux samt Windows XPs inbyggda brandväggar uppfyllde således tjänsteutnyttjandet.

Värt att nämna är Windows Messengers sätt att hantera ICF. Vid utnyttjande av denna tjänst öppnas automatiskt två portar, en TCP och en UDP för att undvika kommunikationsproblem som ICF orsakar. Detta blir än mer tydligt då just ICQ och LICQ inte kan tillgodose vissa av sina tjänster med den inbyggda brandväggen på, till skillnad mot Windows Messenger som klarar detta utmärkt. Användaren blir dock inte meddelad om att de två portarna öppnats ut mot Internet men de är synliga i ICFs konfigurations fönstret, utan att för den delen tala om till vilket program de härrör. Ur ett funktionalitetsperspektiv fungerar detta utmärkt, men innebär även exponering ut mot Internet. Portarna ligger dock i regionen 4.000 till 16.000 och läggs upp slumpvis varje gång Windows Messenger startas på nytt, så att varken användare eller möjligt hot kan förutsäga vilken port som kommer att öppnas härnäst. Automatiskt öppnande av portar blev än mer tydligt när vi utnyttjade fler tjänster som Windows XP erbjöd, så som delande av applikationer och Remote Assistance. Detta innebär att det troligtvis inte dröjer länge innan vi har applikationer som öppnar mer än bara portar i de övre regionerna, utan även tjänsteportar som är känsliga för resursutnyttjande. Remote Assistance är en applikation som ger en användare möjlighet att låta en annan användare se och eventuellt styra dennes dator utifrån. Detta sker genom en extern inloggning via Windows Messenger eller Outlook och parterna kan konversera genom ett chatfönster i realtid.

figur 3. Automatiskt öppnande av portar i ICF.

De flesta tjänster som utnyttjades i testet lyckades fullt ut, förutom när ICQ och LICQ tog emot filer eller skulle upprätta en chat med annan användare. Tjänsterna som lyckades innebar allt från fullbordandet av köp, nedladdning av filer och formulär från diverse webbsidor till att hämta och skicka e-post. Vid test av spel, innebar detta att vi valde bort operativsystemet Red Hat Linux på grund av att det inte finns några kommersiella spel för detta operativsystem. De spel vi hittade till Linux var gratis att ladda ner samt kunde jämföras med spel till PC från tidigt 90-tal. Red Hat Linux är inte ämnad för spel och spelmarknaden,

därför valde vi att bortse från detta test för SLCT. Speltestet för ICF bestod av två delar, dels där W-ALPHA agerade server och där den agerade klient. Vid server förnekades all trafik in av ICF i och med att W-ALPHA inte hade initierat någon kommunikation, medan den som klient fungerade fullt ut. Skillnaden här låg i att W-ALPHA gjorde det initiala anropet, och servern lades då till som accepterad trafik genom ICF.

Vad skiljer det två inbyggda brandväggarna åt ur ett operativt perspektiv? ICF arbetar ur ett fast schema att förvägra alla inkommande paket som användaren själv ej har initierat. Detta får innebörden att alla våra skanningstester och nessus skanningen inte fann ett enda säkerhetshål i den inbyggda brandväggen då den var totalt osynlig utifrån Internet. Det är helt klart att ICF skyddar, då våra tester med Nessus mot Windows XP utan inbyggda brandväggen visade på flera allvarliga säkerhetsbrister i operativsystemet [ö].

Red Hats inbyggda brandvägg agerade på ett annorlunda sätt. Redan vid ICMP anropen, visade det sig att Red Hat svarade när högsta säkerhets nivån var inställd, vilket förvånade oss. Detta kunde ej heller ställas in i inställningarna för att förhindras. I och med att man med en ping kan se datorn, utsätter man den för en betydligt större risk än om Red Hat inte hade svarat på ICMP anropet. För att förstå hur Red Hats SLCT agerade, tog vi fram reglerna den följer [ab]. Där kunde vi se vilka IP-adresser som tilläts tillträde som inkommande trafik och att ingen utgående trafik kontrollerades av SLCT. I reglerna anges även att ett ICMP anrop skall skickas om vissa händelser inträffade, exempelvis att någon försökte anropa en icke öppen port med en SYN [aa].

Vidare kunde vi även visa på vilken form av operativsystem som den inbyggda brandväggen arbetade på. Vid operativsystems identifieringen använde nmap i grunden fyra paket för att få svar. Ett SYN, ett ACK, ett PSH+URG+FIN och slutligen ett UDP-paket mot port 300. Gissningen som nmap utförde var att det var en Linux som arbetade på kärnan 2.4 eller högre trots att den bara fick ett RST svar tillbaka på operativsystems identifieringen. Vid anomali skanningarna opererade ICF med samma åtgärder som mot stealth SYN och trevägshandskakningen. Alla paket förvägrades, oavsett typ av anomali. Red Hat Linux inbyggda brandvägg visade här på svagheten genom att svara med RST till BETA på de portar som var stängda och inte alls där porten var öppen. Detta innebar att anomali skanningarna av Red Hat Linux var lika effektiva som en skanning av operativsystemet utan brandvägg, alla portarna den lyssnade på var synliga utåt. Fyodor, nmaps skapare, talar om att Windows operativsystem inte klarar av att hantera anomali-paket [20]. Men i och med att ICF förvägrade alla paket som användaren på operativsystemet inte initierats, gjorde detta ingen skillnad i vårt resultat.

Vad som bör nämnas är att konfigureringen av Red Hat Linux IPTables som SLCT bygger på, är om man besitter kunskapen som krävs, kan formas så att den i stort sett agerar som användaren själv vill, både vad gäller synlighet utåt sett samt öppna portar, tillåtelse eller förnekande av IP-adresser och nätverk. Men detta innebär att man frångår SLCTs striktare regler och konfiguration och då även vår frågeställning i och med att den inte kan kategoriseras som en inbyggd brandvägg längre.

Vilka styrkor och svagheter finns det med respektive inbyggd brandvägg? En nackdel som präglade de båda inbyggda brandväggarna var att inte alla program fungerade i samarbete med dem. Visserligen kanske inte den vanlige användaren använder just det programmet, men det blir ändå en svaghet, då teoretiskt sett, allt en användare gör ska fungera med den

inbyggda brandväggen. För att hitta inställningarna för de båda inbyggda brandväggarna, så ligger de väl dolda för användaren och kan uppfattas svåra att hitta. Det kan till och med vara så att användaren inte ens vet om att det existerar en inbyggd brandvägg då den från början kan vara avstängd i operativsystemet. Under installationen av Windows XP så beror detta på användarens val om brandväggsinställningarna kommer upp eller ej. Om man konfigurerar sitt nätverk under XPs installation, så kommer det en förfrågan om man vill ha den inbyggda brandväggen installerad. En positiv sak med SLCT är att oavsett inställningar under installationen så kommer en förfrågan om den inbyggda brandväggen upp. På detta viset upplyses användaren om att det finns en inbyggd brandvägg och ger valet om han/hon vill utnyttja denna tjänsten. Med SLCT kan man med hjälp av IPTables utöka och anpassa dessa regler utefter sina behov och på så sätt få en mer mångsidig brandvägg. Men som vi tidigare nämn i diskussionen tidigare, innebär detta att man frångår SLCT. I och med att den begränsar konfigurationen samtidigt som dess grund IPTables besitter en stor kapacitet till formbarhet. För vårt resultat ligger detta till last för Red Hat Linux, då det är SLCT vi testat och inte IPTables. Vid konfiguration av SLCTs inställningar, så visas, oavsett vad man tidigare har valt, så är den högsta säkerhetsnivån förvald. Detta innebär att det är omöjligt att se vilka inställningar man har gjort innan, vilket kan försvåra för användaren.

En intressant aspekt av problemet med att den inbyggda brandväggen blockerar vissa tjänster kom från ICF. Många av de program som medföljer XP har ICF egna lösningar på. ICF öppnar således nya portar i regionen 4000 till 16000 så att dessa applikationer kan fungera utan problem. På detta sätt fungerar Windows Messengers alla funktioner, även de funktioner som inte fungerade på liknande applikationer, jämförelsevis ICQ. Det negativa med portöppnandet är att information om detta aldrig når användaren. Det kan diskuteras huruvida detta påverkar exponeringen att få datorn utsatt för intrång. En faktor som styr detta är om användaren har en fast uppkoppling, så är det vanligt att datorn står på länge, vilket kan innebära att portarna är synliga utåt en längre tid än de normalt skulle, vid exempelvis en modem-anslutning. Vi är av den uppfattningen att det inte föreligger någon större risk då dessa nya portar slumpas ut, och dessutom ligger väldigt högt upp, runt port 4000 till 16000. När man skannar med hjälp av nmap så är det förvalt att först skanna alla tjänsteportar 1 till 1024 för att sedan ta de mer använda portarna över 1024.

Red Hat Linux SLCTs allra största svaghet är att den exponeras betydligt mer än Windows XPs ICF, både genom ping samt nmap skanningen. Vad som även blir tydligt i våra tester är SLCTs oförmåga att gömma de öppna portarna. I Nessus skanningen mot L-ALPHA gjorde den inte någon skillnad på om SLCT var igång eller ej. Däremot skyddade den inbyggda brandväggen mot direkta anslutningsförsök men kunde inte stoppa en redan påbörjad förbindelse.

Windows XPs ICF var under samtliga skanningsförsök osynlig i sin exponering, vilket även resulterade i att Nessus inte hittade några säkerhetshål eller öppna portar i operativsystemet. ICF avbröt även en redan påbörjad icke auktoriserad förbindelse.

ICF är framtagen av Microsoft, främst för modem och bredbandsuppkopplingar, det vill säga mer som ett verktyg för användaren, men ska även enligt tillverkaren kunna agera som yttre brandvägg för ett hem med flera användare som delar på en uppkoppling. Samtidigt som de nämner och talar om en applikation som skall skydda mot säkerhets hot från Internet, ger författaren till Microsoft Networking med förlaget Microsoft i ryggen som förslag att om

läsaren vill ha en effektiv brandvägg skall hon inte förlita sig på ICF utan istället ladda ner Zone Alarm och låta denna mjukvarubrandvägg sköta försvaret [4].

En mindre positiv sak med båda dessa inbyggda brandväggar är att ingen av dem reglerar utgående trafik. Detta innebär i praktiken att trojaner, maskar och liknande kan utnyttja systemet om de väl har kommit in bakom den inbyggda brandväggen. Ofta är det användaren som är den svaga länken här och inte brandväggen. I dagsläget är det fortfarande många som inte tänker till en extra gång innan de exempelvis klickar på en bifogad fil som de fått av en vän eller kollega.

ICF har en loggfunktion där användaren kan ställa in om han vill logga den trafik som går mot hans dator, både sådant som förvägras eller tillåts av den. Detta är en funktion som finns möjlig i IPTables, men som ej ingår i SLCT.

7. SLUTSATS

Den hypotes som legat till grund för vårt arbete, har under processens gång både falsifierats och verifierats av oss gång efter annan. Allt beroende på hur vi själva från start såg på de två inbyggda brandväggarna och dess operativsystem, till att under testerna komma till insikt hur det verkligen låg till. Den delen av hypotes som rör användarnas tjänsteutnyttjande anser vi har verifierats genom våra funktionalitetstester. Genom visade resultat och diskussion har detta bevisats.

Det är helt klart att det finns saker som skiljer de två inbyggda brandväggarna åt, främst då vad gäller användarens integritet. Här blottar Red Hat Linux både vilket operativsystem som finns på datorn, vilka portar som är öppna samt att den finns på nätverket. Skillnaden blir avsevärd då man jämför detta med Windows XP som är totalt osynlig utåt sett vid skanning av portar och sökning i nätverk efter aktiva datorer. I och med detta har vi kommit till slutsatsen att de två inbyggda brandväggarna inte i stort är likartade rörande skydd från hot på Internet. I hypotesen hade vi räknat med en viss skillnad, men det som vårt säkerhetstest visade faller inte inom denna ram.

Slutsatsen av arbetet blir således att vi falsifierar hela vår hypotes. Vi anser att det är helheten som gäller, då både funktion och säkerhet hör ihop. Om någon av dem felar påverkar detta således helheten av hypotesen.

8. AVSLUTNING

Detta arbete har gett oss en djupare förståelse för ICF och SLCTs funktionalitet och säkerhet, och så förhoppningsvis även läsaren. Microsofts lösning på inbyggda brandväggen och dess skarpa säkerhet förvånades oss lika mycket som Red Hat Linux motsvarighet ej levde upp till de förväntningar vi hade på den brandväggslösningen. ICF är att rekommendera för PC användaren, som en enligt oss utmärkt lösning för den som inte har en brandvägg installerad eller funderar på att installera Windows XP. Red Hat användaren bör istället förlita sig helt på att konfigurera upp en egen mjukvarubrandvägg via IPTables.

En idé som har utvecklats under arbetets gång, så består en brandvägg av tre olika faktorer som står i relation till varandra. Säkerhet, det vill säga hur pass säker brandväggen egentligen är, Funktionaliteten det vill säga hur pass väl brandväggen passar in bland övrig programvara på en dator, samt Användarvänligheten, här ingår bland annat manualkvalitet, support från leverantörer, konfigurationssvårigheter och liknande. Om man inkluderar användarvänligheten i analyseringen så kommer man att få en mer övergripande bild över hur den totala brandväggens användbarhet är. Dessa tankar skulle kunna vara av intresse att undersöka i vidare studier eller förslag som uppsatsämne.

Andra vägval som man kunde ha gjort under arbetets gång var att studera ytterligare en brandvägg, nämligen en kommersiell brandvägg, exempelvis Zone Alarm. Det hade varit intressant att se hur de inbyggda brandväggarna står sig mot kommersiella brandväggar och genomdriva vår hypotes och frågeställning även på dessa.

Kritik mot den metoden vi använt oss av kan vara att vi i stort har undvikit att beröra operativsystemen bakom de två inbyggda branväggarna. I och med att de bidrar både till stabilitet men likaledes många svagheter och instabilitet i det totala systemet där brandväggen ingår. Möjligt är att de inbyggda brandväggarna och operativsystemen står i en betydligt större relation och beroende än vad vår studie har visat. Detta ligger dock utanför vår avgränsning, även om det i viss mån kan ha påverkat vissa delar av funktionalitetstestet.

9. KÄLLFÖRTECKNING

[1] Matthew & Perkins, Charles Strebe, *Brandväggar 24sju*, 2:a upplagan, Network Press 2002.

[2] Bill McCarty, *Red Hat Linux Firewalls*, Wiley Publishing, 2003.

[3] C. Pfleegeer, S. Pfleeger, *Security in Computing*, Third Edition, Prentice-Hall Inc, 2003.

[4] Curt Simmons with James Causeyÿ, *Microsoft Windows XP Networking inside out*, Microsoft Press, 2003.

[5] Anonymous, *Maximum Security*, 3:e upplagan, Sams Publishing, May 2001.

[6] W. Stallings, *Operating Systems - Internals and Design Principles*, 4th edition, Prentice-Hall Inc, 2001.

[7] W. Stallings, *Local & Metropolitan Area Networks* 6th Edition, Prentice-Hall Inc, 2000.

[8] J. Postel, *792 Internet Control Message Protocol*, Semptember 1981.

[9] J. Postel, *1340 Assigned Numbers* J. Reynolds, July 1992.

[10] J. Postel, *791 Internet Protocol*, September 1981.

[11] J. Postel, *793 Transport Control Protocol*, September 1981.

[12] J. Postel, *768 User Datagram Protocol*, Augusti 1980.

[13] Firewall Tool Kit. http://www.fwtk.org

[14] Trusted Information Systems. http://www.tis.com

[15] Checkpoint. http://www.checkpoint.com

[16] Red Hat Linux. http://www.redhat.com

[17] IDG. http://www.idg.com

[18] Microsoft Inc.
http://www.microsoft.com/windowsxp/pro/techinfo/planning/techoverview/

[19] Microsoft Inc. Om Internet Connection Firewall.
http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/hnw_understanding_firewall.asp

[20] Nmap 3.27. http://www.insecure.org/nmap/

[21] Nessus 2.0. http://www.nessus.org/

[22] Tcpdump. http://www.tcpdump.org/

[23] Windump. http://windump.polito.it/

[24] Netcat 1.1. http://www.atstake.com/research/tools/network_utilities/

[25] National Institute of Standards and Technology Special Publication 800-42
http://csrc.nist.gov/publications/drafts/security-testing.pdf,
Natl. Inst. Stand. Technol. Spec. Publ. 800-42, XX pages (Feb. 2002).

[26] Elisabeth Olinder och Mari Petterson, *Datasäkerhet för hemdatorer, brandväggar för privatpersoner*, Blekinge Tekniska Högskola, IPD, ht 2001.

[27] SCBs undersökning, Privatpersoners användning av datorer och Internet 2002.
http://www.scb.se/publkat/Filer/TKFT0302.pdf

APPENDIX A

I denna bilaga ligger först Säkerhetstesterna med utdrag från ICF-loggar, Windump samt Tcpdump. Därefter följer resultaten från Funktionalitetstestet med utdrag från rapporterna från Windump och Tcpdump. Avslutningsvis Nessus rapporter och brandväggs regler / agerande följt av Applikations versioner samt SCB frågan för grunden till Funktionalitetstestet.

Säkerhetstestet:

[a] Sammanställning säkerhetstester utan inbyggda brandvägg:

Skanning	W-ALPHA	L-ALPHA
ping	reply	reply
OS-identifikation	Me, Win2k, XP	Kernel 2.4.0 – 2.5.20
3vägshandskakning	accept	accept
stealth SYN	accept	accept
Anomalier	ej applicerbart	accept
Fragmenterat	-	-
Spoof	ej applicerbart	ej applicerbart
UDP-skanning	accept	accept
Idle-skanning	accept	ej applicerbart
Nessus	se [ö]	samma som med brandvägg påslagen
Netcat	accept	accept

[b] Sammanställning säkerhetstest med inbyggd brandvägg på:

Skanning	W-ALHPA	L-ALPHA
ping	drop	reply
OS-identifikation	drop	less reliable Kernel 2.4 -2.5.x
3vägshandskakning	drop	drop
stealth SYN	drop	drop
Anomalier	drop	RST+ACK, drop
Fragmenterat	ingen skillnad	ingen skillnad
Spoof	drop	drop funkade inte
UDP-skanning	drop	drop
Idle-skanning	drop	ej applicerbart
Nessus	se [ä]	se [å]
Netcat	drop	drop

[c] L-ALPHA öppna portar:

verktyg: netstat
TCP 22, 111, 1024, 6000
UDP 111, 1024

[d] W-ALPHA öppna portar:

verktyg: netstat
TCP 135, 445, 1025, 1027, 5000, 139
UDP 123, 135, 137, 138, 445, 500, 1900, 2234

[e] W-ALPHA UDP och TCP skanning med Nmap:

Kontroll av W-ALPHA utan brandvägg, inga Internet applikationer igång.

Interesting ports on 194.47.139.62:
(The 3069 ports scanned but not shown below are in state: closed)
Port State Service
123/udp open ntp
135/tcp open loc-srv
135/udp open loc-srv

137/udp open netbios-ns
138/udp open netbios-dgm
139/tcp open netbios-ssn
445/tcp open microsoft-ds
445/udp open microsoft-ds
500/udp open isakmp
1025/tcp open NFS-or-IIS
1900/udp open UPnP
5000/tcp open UPnP
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP

[f] L-ALPHA UDP och TCP skanning med Nmap utan brandvägg:

Interesting ports on 194.47.139.62:
(The 3088 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
111/tcp open sunrpc
111/udp open sunrpc
1024/tcp open kdm
1024/udp open unknown
6000/tcp open X11
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20

[g] Ping på L-ALPHA med SLCT:

PING 194.47.139.62 (194.47.139.62) from 194.47.139.63 : 56(84) bytes of data.
64 bytes from 194.47.139.62: icmp_seq=1 ttl=64 time=0.297 ms
64 bytes from 194.47.139.62: icmp_seq=2 ttl=64 time=0.246 ms

tcpdump:
11:55:58.421103 194.47.139.63 > 194.47.139.62: icmp: echo request (DF)
11:55:58.421199 194.47.139.62 > 194.47.139.63: icmp: echo reply

[h] Ping på W-ALPHA med ICF:

windump:
12:44:38.700762 IP 194.47.139.63 > Alpha: icmp 64: echo request seq 3072 (DF)
12:44:39.702871 IP 194.47.139.63 > Alpha: icmp 64: echo request seq 3328 (DF)

ICF logg:
2003-04-28 15:11:39 DROP ICMP 194.47.139.63 194.47.139.62 - - 84 - - - - 8 0 -
2003-04-28 15:11:40 DROP ICMP 194.47.139.63 194.47.139.62 - - 84 - - - - 8 0 -

[i] W-ALPHA operativsystems identifiering:

Nmap:
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
Too many fingerprints match this host for me to give an accurate OS guess

ICF-logg:
2003-04-28 18:25:22 DROP TCP 194.47.139.63 194.47.139.62 61943 53 40 S 538482110 0 2048 - - -
2003-04-28 18:25:28 DROP TCP 194.47.139.63 194.47.139.62 61949 38838 60 S 2347040856 0 2048 - - -
2003-04-28 18:25:28 DROP TCP 194.47.139.63 194.47.139.62 61950 38838 60 A 2347040856 0 2048 - - -
2003-04-28 18:25:28 DROP TCP 194.47.139.63 194.47.139.62 61951 38838 60 FUP 2347040856 0 2048 - - -
2003-04-28 18:25:28 DROP UDP 194.47.139.63 194.47.139.62 61938 38838 328 - - - - - - -

windump:
12:55:11.371405 IP 194.47.139.63.59415 > Alpha.41879: S 1144604389:1144604389(0) win 1024 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
12:55:11.371533 IP 194.47.139.63.59416 > Alpha.41879: . ack 1 win 1024 <wscale 10,nop,mss 265,timestamp 061109567 0,eol>
12:55:11.371555 IP 194.47.139.63.59417 > Alpha.41879: FP 1144604389:1144604389(0) win 1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
12:55:11.371592 IP 194.47.139.63.59404 > Alpha.41879: udp 300

[j] L-ALPHA operativsystems identifiering:

Nmap:
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open an
d 1 closed TCP port
All 1611 scanned ports on 194.47.139.62 are: filtered
Remote OS guesses: Linux Kernel 2.4.0 - 2.5.20, Linux Kernel 2.4.0 - 2.5.20 w/o tcp_timestam
ps, Linux kernel 2.4.18 - 2.4.20 (X86), Gentoo 1.2 linux (Kernel 2.4.19-gentoo-rc5), Linux 2

.4.18 - 2.4.20 (X86), Linux 2.4.19 w/grsecurity patch, Linux 2.5.25 - 2.5.59 or Gentoo 1.2 L
inux 2.4.19 rc1-rc7), Linux 2.4.7 (X86)

tcpdump:
20:17:56.086137 194.47.139.63.45603 > 194.47.139.62.34076: S 347972143:347972143(0) win 4096 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
20:17:56.086402 194.47.139.62 > 194.47.139.63: icmp: 194.47.139.62 tcp port 34076 unreachable [tos 0xc0]
20:17:56.194216 194.47.139.63.45604 > 194.47.139.62.34076: . ack 0 win 4096 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
20:17:56.194424 194.47.139.62.34076 > 194.47.139.63.45604: R 0:0(0) win 0 (DF)
20:17:56.329746 194.47.139.63.45605 > 194.47.139.62.34076: FP 347972143:347972143(0) win 4096 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567 0,eol>
20:17:56.329916 194.47.139.62.34076 > 194.47.139.63.45605: R 0:0(0) ack 347972144 win 0 (DF)
20:17:56.446411 194.47.139.63.45592 > 194.47.139.62.34076: udp 300
20:17:56.446732 194.47.139.62 > 194.47.139.63: icmp: 194.47.139.62 udp port 34076 unreachable [tos 0xc0]

[k] W-ALPHA trevägs handskakning:

nmap:
All 1623 scanned ports on 194.47.139.62 are: filtered

ICF-logg:
2003-04-28 16:06:01 DROP TCP 194.47.139.63 194.47.139.62 4385 63000 60 S 4287405228 0 5840 - - -
2003-04-28 16:06:01 DROP TCP 194.47.139.63 194.47.139.62 4386 54 60 S 4284593973 0 5840 - - -

windump:
13:00:56.312271 IP 194.47.139.63.2310 > Alpha.139: S 1393990124:1393990124(0) win 5840 <mss 1460,sackOK,timestamp 44567714 0,nop,wscale 0> (DF)
13:00:56.312403 IP 194.47.139.63.2311 > Alpha.135: S 1389452850:1389452850(0) win 5840 <mss 1460,sackOK,timestamp 44567714 0,nop,wscale 0> (DF)

[l] L-ALPHA trevägs handskakning:

nmap:
All 1623 scanned ports on 194.47.139.62 are: filtered

tcpdump:
11:58:02.720508 194.47.139.63.1431 > 194.47.139.62.577: S 1722609219:1722609219(0) win 5840 <mss 1460,sackOK,timestamp 42635492 0,nop,wscale 0> (DF)
11:58:02.720593 194.47.139.62 > 194.47.139.63: icmp: 194.47.139.62 tcp port 577 unreachable [tos 0xc0]
11:58:02.720572 194.47.139.63.1432 > 194.47.139.62.4500: S 1722066565:1722066565(0) win 5840 <mss 1460,sackOK,timestamp 42635492 0,nop,wscale 0> (DF)

[m] W-ALPHA SYN stealth skanning:

nmap:
All 64000 scanned ports on 194.47.139.62 are: filtered

ICF-logg:
2003-04-05 14:59:14 DROP TCP 194.47.139.63 194.47.139.62 13861 1 40 S 1678464923 0 4096 - - -
2003-04-05 14:59:14 DROP TCP 194.47.139.63 194.47.139.62 13862 110 40 S 1678464923 0 2048 - - -

windump:
13:03:55.677001 IP 194.47.139.63.60710 > Alpha.80: S 1016563578:1016563578(0) win 3072
13:03:55.677021 IP 194.47.139.63.60710 > Alpha.11865: S 1016563578:1016563578(0) win 3072

[n] L-ALPHA SYN stealth scanning:

nmap:
All 1623 scanned ports on 194.47.139.62 are: filtered

Tcpdump:
12:00:21.931404 194.47.139.63.39229 > 194.47.139.62.cmip-agent: S 1203921304:1203921304(0) win 1024
12:00:21.931438 194.47.139.63.39229 > 194.47.139.62.951: S 1203921304:1203921304(0) win 3072
12:00:21.931473 194.47.139.63.39229 > 194.47.139.62.rlp: S 1203921304:1203921304(0) win 3072

[o] W-ALPHA anomali paket - stealth FIN skanning:

nmap:
All 1623 scanned ports on 194.47.139.62 are: filtered

windump:
13:09:03.088465 IP 194.47.139.63.55396 > Alpha.943: F 0:0(0) win 2048
13:09:03.088496 IP 194.47.139.63.55396 > Alpha.310: F 0:0(0) win 2048

ICF-logg:
2003-04-28 15:57:39 DROP TCP 194.47.139.63 194.47.139.62 39810 5000 40 F 0 0 3072 - - -
2003-04-28 15:57:39 DROP TCP 194.47.139.63 194.47.139.62 39810 1024 40 F 0 0 3072 - - -

[p] L-ALPHA anomali paket – stealth FIN skanning:

nmap:
Interesting ports on 194.47.139.62:
(The 1607 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
111/tcp open sunrpc
1024/tcp open kdm
6000/tcp open X11

tcpdump:
12:04:11.462014 194.47.139.63.39584 > 194.47.139.62.46: F 0:0(0) win 2048
12:04:11.462031 194.47.139.62.46 > 194.47.139.63.39584: R 0:0(0) ack 1 win 0 (DF)
12:04:11.763009 194.47.139.63.39585 > 194.47.139.62.ssh: F 0:0(0) win 4096
12:04:11.763049 194.47.139.63.39585 > 194.47.139.62.x11: F 0:0(0) win 4096

[q] W-ALPHA anonamli paket - stealth X-mas skanning:

ICF-logg:
2003-04-28 16:01:37 DROP TCP 194.47.139.63 194.47.139.62 49347 5000 40 FUP 0 0 4096 - - -
2003-04-28 16:01:37 DROP TCP 194.47.139.63 194.47.139.62 49347 563 40 FUP 0 0 4096 - - -

windump:
13:11:11.371555 IP 194.47.139.63.59417 > Alpha.5000: FP 1143304389:1143304389(0) win 1024 urg 0 <wscale 10,nop,mss 265,timestamp 1061145567 0,eol>

[r] L-ALPHA anomali paket – stealth X-mas skanning:

nmap:
Interesting ports on 194.47.139.62:
(The 1607 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
111/tcp open sunrpc
1024/tcp open kdm
6000/tcp open X11

tcpdump:
12:05:27.150952 194.47.139.63.35993 > 194.47.139.62.ssh: FP 0:0(0) win 3072 urg 0
12:05:27.150992 194.47.139.63.35993 > 194.47.139.62.re-mail-ck: FP 0:0(0) win 3072 urg 0
12:05:27.151109 194.47.139.62.re-mail-ck > 194.47.139.63.35993: R 0:0(0) ack 1 win 0 (DF)

[s] W-ALPHA anomali paket – stealth NULL skanning:

ICF-logg:
2003-04-28 19:54:59 DROP TCP 194.47.139.63 194.47.139.62 51064 5000 40 - 0 0 4096 - - -
2003-04-28 19:54:59 DROP TCP 194.47.139.63 194.47.139.62 51064 53 40 - 0 0 4096 - - -

windump:
13:12:24.397304 IP 194.47.139.63.55634 > Alpha.431: . win 3072
13:12:24.397339 IP 194.47.139.63.55634 > Alpha.208: . win 1024

[t] L-ALPHA anomali paket – stealth NULL skanning:

Nmap:
Interesting ports on 194.47.139.62:
(The 1607 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
111/tcp open sunrpc
1024/tcp open kdm
6000/tcp open X11

tcpdump:
12:08:24.140473 194.47.139.63.63815 > 194.47.139.62.http: . win 3072
12:08:24.140541 194.47.139.62.http > 194.47.139.63.63815: R 0:0(0) ack 0 win 0 (DF)
12:08:24.450131 194.47.139.63.63816 > 194.47.139.62.1024: . win 4096
12:08:24.450173 194.47.139.63.63816 > 194.47.139.62.ssh: . win 3072

[u] W-ALPHA fragmenterad stealth SYN:

ICF-logg:
2003-04-28 18:22:16 DROP TCP 194.47.139.63 194.47.139.62 63020 53 40 S 1021900536 0 2048 - - -
2003-04-28 18:22:22 DROP TCP 194.47.139.63 194.47.139.62 63021 5000 40 S 3477287674 0 2048 - - -

windump:
13:14:22.714063 IP 194.47.139.63 > Alpha: tcp (frag 25263:4@16)
13:14:22.714086 IP 194.47.139.63.52776 > Alpha.28: S [bad hdr length] (frag 59010:16@0+)
13:14:22.714096 IP 194.47.139.63 > Alpha: tcp (frag 59010:4@16)
13:14:22.714141 IP 194.47.139.63.52776 > Alpha.1003: S [bad hdr length] (frag 39575:16@0+)

[v] L-ALPHA fragmenterad stealth SYN:

nmap:
Host 194.47.139.62 appears to be up ... good.
Initiating SYN Stealth Scan against 194.47.139.62 at 11:24
The SYN Stealth Scan took 20 seconds to scan 1611 ports.
All 1611 scanned ports on 194.47.139.62 are: filtered

Tcpdump:
12:12:10.080873 194.47.139.63.40879 > 194.47.139.62.241: S [bad hdr length] (frag 51738:16@0+)
12:12:10.080900 194.47.139.63 > 194.47.139.62: (frag 51738:4@16)
12:12:10.080933 194.47.139.63.40879 > 194.47.139.62.canna: S [bad hdr length] (frag 62803:16@0+)
12:12:10.080978 194.47.139.63 > 194.47.139.62: (frag 62803:4@16)

[w] W-ALPHA idle skanning:

nmap:
[kommando: nmap -P0 -sI 194.47.139.62 www.dn.se]
Idlescan zombie 194.47.139.62 (194.47.139.62) port 80 cannot be used because IPID sequencability class is: Busy server or unknown class. Try another proxy.
QUITTING!

tcpdump från BETA:
18:47:17.473093 194.47.139.63.49684 > 194.47.139.62.http: S 2034723409:2034723409(0) ack 0 win 64447
18:47:17.564890 194.47.139.63.49685 > 194.47.139.62.http: S 2034723410:2034723410(0) ack 0 win 64447

ICF-logg:
2003-04-06 14:08:21 DROP TCP 194.47.139.63 194.47.139.62 14645 80 40 SA 651531721 0 46365 - - -
2003-04-06 14:08:21 DROP TCP 194.47.139.63 194.47.139.62 14646 80 40 SA 651531722 0 46365 - - -

[x] W-ALPHA UDP skanning:

All 1471 scanned ports on 194.47.139.62 are: filtered

ICF-logg:
2003-04-28 19:59:17 DROP UDP 194.47.139.63 194.47.139.62 47708 53 28 - - - - - - -
2003-04-28 19:59:17 DROP UDP 194.47.139.63 194.47.139.62 47708 80 28 - - - - - - -

windump:
13:16:22.515524 IP 194.47.139.63.55936 > Alpha.131: udp 0
13:16:22.515564 IP 194.47.139.63.55936 > Alpha.136: udp 0

[y] L-ALPHA UDP skanning:

tcpdump:
12:17:33.173078 194.47.139.63.48219 > 194.47.139.62.sunrpc: udp 0
12:17:33.173152 194.47.139.62 > 194.47.139.63: icmp: 194.47.139.62 udp port sunrpc unreachable [tos 0xc0]

[z] W-ALPHA utan ICF idle skanning:

Idlescan using zombie 194.47.139.62 (194.47.139.62:80); Class: Incremental
Interesting ports on (213.132.113.2):
(The 1592 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
...

tpcdump:
18:53:19.347181 194.47.139.62.http > 213.132.113.2.domain: S 1527107969:1527107969(0) win 1024
18:53:19.347211 194.47.139.62.http > 213.132.113.2.796: S 1527107969:1527107969(0) win 1024
18:53:19.399145 194.47.139.63.56205 > 194.47.139.62.http: S 273299107:273299107(0) ack 22291449 win 1024
18:53:19.399438 194.47.139.62.http > 194.47.139.63.56205: R 22291449:22291449(0) win 0

[A] W-ALPHA netcat:

Utan brandvägg:
14:59:13.065838 IP 194.47.139.63.1033 > Alpha.53: S 1325948620:1325948620(0) win 5840 <mss 1460,sackOK,timestamp 345792 0,nop,wscale 0> (DF)
14:59:13.065987 IP Alpha.53 > 194.47.139.63.1033: S 4262977409:4262977409(0) ack 1325948621 win 64240 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF)
14:59:13.066223 IP 194.47.139.63.1033 > Alpha.53: . ack 1 win 5840 <nop,nop,timestamp 345792 0> (DF)

ICF på port 53:
windump:
15:03:10.410405 IP 194.47.139.63.1034 > Alpha.53: S 1573487288:1573487288(0) win 5840 <mss 1460,sackOK,timestamp 467337 0,nop,wscale 0> (DF)

ICF logg:
2003-05-08 15:03:55 DROP TCP 194.47.139.63 194.47.139.62 1034 53 60 S 1573487288 0 5840 - - -

på öppen port (5190) men stängd av ICF:
ICF logg:
2003-05-08 15:06:29 DROP TCP 194.47.139.63 194.47.139.62 1036 5190 60 S 1805431653 0 5840 - - -
2003-05-08 15:06:32 DROP TCP 194.47.139.63 194.47.139.62 1036 5190 60 S 1805431653 0 5840 - - -

windump:
15:06:29.642470 IP 194.47.139.63.1036 > Alpha.5190: S 1805431653:1805431653(0) win 5840 <mss 1460,sackOK,timestamp 569361 0,nop,wscale 0> (DF)

Öppen port i ICF 6110:
windump:
15:10:22.233657 IP 194.47.139.63.1037 > Alpha.6110: S 2034740689:2034740689(0) win 5840 <mss 1460,sackOK,timestamp 688473 0,nop,wscale 0> (DF)
15:10:22.234148 IP Alpha.6110 > 194.47.139.63.1037: S 135500686:135500686(0) ack 2034740690 win 64240 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF)
15:10:22.234342 IP 194.47.139.63.1037 > Alpha.6110: . ack 1 win 5840 <nop,nop,timestamp 688474 0> (DF)

Brandväggen först inte igång, därefter sattes den på:
ICF-loggning:
2003-05-10 19:25:21 DROP TCP 194.47.139.63 194.47.139.62 1372 12 56 AP 2974661606 1667533603 14480 - - -
2003-05-10 19:25:21 DROP TCP 194.47.139.63 194.47.139.62 1372 12 56 AP 2974661606 1667533603 14480 - - -

tcpdump från BETA:
19:25:56.965566 194.47.139.63.1372 > 194.47.139.62.12: P 71:75(4) ack 94505 win 14480 <nop,nop,timestamp 96997363 9750> (DF)
19:25:58.715576 194.47.139.63.1372 > 194.47.139.62.12: P 71:75(4) ack 94505 win 14480 <nop,nop,timestamp 96998259 9750> (DF)

[B] L-ALPHA netcat:

Ingen brandvägg på.
[root@ALPHA installed]# ./nc -l -p 53 -v -e /bin/sh
listening on [any] 53 ...
194.47.139.63: inverse host lookup failed: Unknown host
connect to [194.47.139.62] from (UNKNOWN) [194.47.139.63] 1195

tcpdump:
16:07:29.738400 194.47.139.63.1195 > 194.47.139.62.domain: S 1375232537:1375232537(0) win 5840 <mss 1460,sackOK,timestamp 2443505 0,nop,wscale 0> (DF)
16:07:29.738515 194.47.139.62.domain > 194.47.139.63.1195: S 3418687828:3418687828(0) ack 1375232538 win 5792 <mss 1460,sackOK,timestamp 1572226 2443505,nop,wscale 0> (DF)
16:07:29.738705 194.47.139.63.1195 > 194.47.139.62.domain: . ack 1 win 5840 <nop,nop,timestamp 2443505 1572226> (DF)

SLCT på vid öppen port som endast tillåter trafik till DNS
tcpdump:
16:13:56.706944 194.47.139.63.1026 > 194.47.139.62.domain: 27763 inv_q [b2&3=0xa00] [0a] (3) (DF)
16:13:56.707023 194.47.139.62 > 194.47.139.63: icmp: 194.47.139.62 udp port domain unreachable [tos 0xc0]

SLCT på vid öppen port som tillåts.
tcpdump:
6:11:47.689133 194.47.139.63.1198 > 194.47.139.62.http: S 1648346383:1648346383(0) win 5840 <mss 1460,sackOK,timestamp 2575578 0,nop,wscale 0> (DF)
16:11:47.689247 194.47.139.62.http > 194.47.139.63.1198: S 3686704446:3686704446(0) ack 1648346384 win 5792 <mss 1460,sackOK,timestamp 1704297 2575578,nop,wscale 0> (DF)
16:11:47.689448 194.47.139.63.1198 > 194.47.139.62.http: . ack 1 win 5840 <nop,nop,timestamp 2575578 1704297> (DF)

SLCT av vid uppkoppling mot ALPHA, därefter sattes den på.
tcpdump:

18:45:04.056542 194.47.139.63.1369 > 194.47.139.62.domain: P 3:6(3) ack 120 win 5840 <nop,nop,timestamp 95759296 94870737> (DF)
18:45:04.056789 194.47.139.62.domain > 194.47.139.63.1369: . ack 6 win 5792 <nop ,nop,timestamp 94886437 95759296> (DF)
18:45:04.176182 194.47.139.62.domain > 194.47.139.63.1369: P 120:239(119) ack 6 win 5792 <nop,nop,timestamp 94886498 95759296> (DF)

[root@ALPHA installed]# ./nc -l -p 53 -v -e /bin/sh
listening on [any] 53 ...
194.47.139.63: inverse host lookup failed: Unknown host
connect to [194.47.139.62] from (UNKNOWN) [194.47.139.63] 1369

Kommunikationen fortsatte och vi kunde skapa kataloger eller ta bort filer ävenefter att brandväggen slagits på. Det hade inte varit några problem här att lägga till en regel i IPTables för att öppna en port konstant.

[C] W-ALPHA spoofed:

spoofed sender nmap:
2003-04-06 14:49:30 DROP TCP 195.67.71.113 194.47.139.62 56592 5000 40 S 3616010187 0 4096 - - -
2003-04-06 14:49:30 DROP TCP 195.67.71.113 194.47.139.62 56592 4995 40 S 3616010187 0 3072 - - -
2003-04-06 14:49:30 DROP TCP 195.67.71.113 194.47.139.62 56592 4998 40 S 3616010187 0 3072 - - -

den äkta IP-adressen som hade tillåtelse att ta sig in genom ICF:
2003-04-06 14:49:32 OPEN TCP 194.47.139.62 195.67.71.113 4819 80 - - - - - - - -
2003-04-06 14:49:32 OPEN TCP 194.47.139.62 195.67.71.113 4820 80 - - - - - - - -
2003-04-06 14:49:32 OPEN TCP 194.47.139.62 195.67.71.113 4821 80 - - - - - - - -

[D] L-ALPHA spoofed:

spoofad DNS, STCF svarade inte med ett ICMP anrop vid udp skanning från spoofad DNS. Dock så kunde inte nmap tillgodo se sig detta resultatet. Troligast har detta med att DNS:n cymbal.bth.se är konfigurerad för att inte föra vidare spoofade paket.

Tcpdump:
19:02:07.319943 cymbal.bth.se.domain > 194.47.139.62.sunrpc: 0 [0q] (0)
19:02:07.319986 cymbal.bth.se.domain > 194.47.139.62.112: 0 [0q] (0)
19:02:07.320062 194.47.139.62 > cymbal.bth.se: icmp: 194.47.139.62 udp port 112 unreachable [tos 0xc0]

[å] Nessus Scan Report L-ALPHA

SUMMARY
- Number of hosts which were alive during the test : 1
- Number of security holes found : 0
- Number of security warnings found : 1
- Number of security notes found : 7

TESTED HOSTS
194.47.139.62 (Security warnings found)

DETAILS
+ 194.47.139.62 :
. List of open ports :
o ssh (22/tcp) (Security notes found)
o ssh (22/udp)
o sunrpc (111/tcp) (Security notes found)
o sunrpc (111/udp)
o kdm (1024/tcp) (Security notes found)
o x11 (6000/tcp) (Security notes found)
o general/tcp (Security notes found)
o general/icmp (Security warnings found)
o general/udp (Security notes found)

. Information found on port ssh (22/tcp)
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by some
information gathering plugin

. Information found on port sunrpc (111/tcp)
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by some
information gathering plugin

. Information found on port kdm (1024/tcp)
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by some

information gathering plugin

. Information found on port x11 (6000/tcp)
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by some
information gathering plugin

. Information found on port general/tcp

HTTP NIDS evasion functions are enabled.
You may get some false negative results

. Information found on port general/tcp
Nmap found that this host is running Linux Kernel 2.4.0 - 2.5.20, Linux
2.4.19-pre4 on Alpha, Linux Kernel 2.4.0 - 2.5.20 w/o tcp_timestamps,
Gentoo 1.2 linux (Kernel 2.4.19-gentoo-rc5), Linux 2.5.25 or Gentoo 1.2
Linux 2.4.19 rc1-rc7), Linux 2.4.7 (X86)

. Warning found on port general/icmp
The remote host answers to an ICMP timestamp
request. This allows an attacker to know the
date which is set on your machine.

This may help him to defeat all your
time based authentication protocols.

Solution : filter out the ICMP timestamp
requests (13), and the outgoing ICMP
timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

. Information found on port general/udp

For your information, here is the traceroute to 194.47.139.62 :
194.47.139.62

This file was generated by the Nessus Security Scanner

[ä] Nessus Scan Report W-ALPHA

SUMMARY
- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 0
- Number of security notes found : 1

TESTED HOSTS
194.47.139.62 (Security holes found)

DETAILS
+ 194.47.139.62 :
. List of open ports :
o general/tcp (Security hole found)

. Vulnerability found on port general/tcp :

It was possible to crash the remote
system using the 'oshare' attack.

An attacker may use this problem
to prevent your site from working
properly.

Solution : contact your vendor for
a patch.

Risk factor : Serious
CVE : CVE-1999-0357

. Information found on port general/tcp

HTTP NIDS evasion functions are enabled.
You may get some false negative results

This file was generated by the Nessus Security Scanner

[ö] Nessus skanning W-ALPHA utan ICF igång:

SUMMARY
- Number of hosts which were alive during the test : 1
- Number of security holes found : 6
- Number of security warnings found : 4
- Number of security notes found : 9

TESTED HOSTS
194.47.139.62 (Security holes found)

DETAILS
+ 194.47.139.62 :
. List of open ports :
o loc-srv (135/tcp) (Security hole found)
o netbios-ssn (139/tcp) (Security warnings found)
o microsoft-ds (445/tcp)
o NFS-or-IIS (1025/tcp) (Security notes found)
o UPnP (5000/tcp) (Security hole found)
o general/tcp (Security warnings found)
o unknown (1027/udp) (Security notes found)
o general/icmp (Security warnings found)
o general/udp (Security notes found)

Funktionalitets test:

[E] Sammanställing funktionalitets testet:

Applikation		Windows XP ICF	Red Hat 8.0
Windows Messenger/Gaim			
	Skicka meddelande	lyckat	lyckat
	Skicka fil	lyckat	finns ej
	Ta emot fil	lyckat	finns ej
	Chat	lyckat	lyckat
ICQ/LICQ			
	Skicka meddelande	lyckat	lyckat
	Skicka fil	lyckat	lyckat
	Ta emot fil	misslyckat	misslyckat
	Chat	misslyckat	finns ej
Outlook/Ximian			
	Skicka e-post	lyckat	lyckat
	Ta emot e-post	lycka	lyckat
	Nyhetsgrupper	lyckat	lyckat
Webmail (IMAP)			
	Skicka e-post	lyckat	lyckat
	Ta emot e-post	lyckat	lyckat
IRC		lyckat	lyckat
Sökningar		lyckat	lyckat
Spel			
	Klient	lyckat	finns ej
	Server	misslyckat	finns ej
Mediaspelare		lyckat	lyckat
Nedladdning			
	FTP	lyckat	lyckat
	http	lyckat	lyckat
Formulär			
	Nedladdning	se http nedladdning	
	Läsning	se http nedladdning	
Köp & Sälj			
Internet bank		lyckat	lyckat
Beställning av vara		lyckat	lyckat

[F] ICQ för Windows XP

Skicka meddelande:
18:58:04.152823 IP Alpha.3432 > h29n3c1o1031.bredband.skanova.com.3234: P 53:55(2) ack 88 win 63956 (DF)
18:58:04.302552 IP h29n3c1o1031.bredband.skanova.com.3234 > Alpha.3432: . ack 55 win 64726 (DF)

Skicka fil:
10:48:08.717478 IP Alpha.3922 > EPSILON.12665: S 81300060:81300060(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
10:48:08.717787 IP EPSILON.12665 > Alpha.3922: S 2373475:2373475(0) ack 81300061 win 8760 <mss 1460> (DF)
10:48:08.717891 IP Alpha.3922 > EPSILON.12665: . ack 1 win 64240 (DF)
10:48:08.724395 IP Alpha.3922 > EPSILON.12665: P 1:3(2) ack 1 win 64240 (DF)
10:48:08.901805 IP EPSILON.12665 > Alpha.3922: . ack 3 win 8758 (DF)

Ta emot fil:
2003-04-08 19:04:35 DROP TCP 213.65.34.29 194.47.139.62 4151 19013 48 S 3617396469 0 65340 - - -
2003-04-08 19:04:38 DROP TCP 213.65.34.29 194.47.139.62 4151 19013 48 S 3617396469 0 65340 - - -
2003-04-08 19:04:44 DROP TCP 213.65.34.29 194.47.139.62 4151 19013 48 S 3617396469 0 65340 - - -

Ta emot fil utan ICF :
18:40:42.295105 IP Alpha.3143 > h100n5c1o1031.bredband.skanova.com.3389: P 17:104(87) ack 110 win 64123 (DF)
18:40:42.410298 IP Alpha.3143 > h100n5c1o1031.bredband.skanova.com.3389: P 104:191(87) ack 110 win 64123 (DF)
18:40:42.438987 IP h100n5c1o1031.bredband.skanova.com.3389 > Alpha.3143: . ack 191 win 64879 (DF)

Chat
2003-04-09 18:32:23 DROP TCP 213.101.59.173 194.47.139.62 1103 10745 48 S 1353060 0 8192 - - -
2003-04-09 18:32:23 DROP TCP 213.101.59.173 194.47.139.62 1104 10745 48 S 1353064 0 8192 - - -
2003-04-09 18:32:23 DROP TCP 213.101.59.173 194.47.139.62 1105 10745 48 S 1353067 0 8192 - - -
2003-04-09 18:32:26 DROP TCP 213.101.59.173 194.47.139.62 1105 10745 48 S 1353067 0 8192 - - -
2003-04-09 18:32:26 DROP TCP 213.101.59.173 194.47.139.62 1104 10745 48 S 1353064 0 8192 - - -
2003-04-09 18:32:26 DROP TCP 213.101.59.173 194.47.139.62 1103 10745 48 S 1353060 0 8192 - - -

Chat utan ICF:
18:36:01.267302 IP Alpha.3143 > h100n5c1o1031.bredband.skanova.com.3389: P 858:875(17) ack 9433 win 65340 (DF)
18:36:01.342013 IP h100n5c1o1031.bredband.skanova.com.3389 > Alpha.3143: P 9433:10078(645) ack 875 win 64640 (DF)
18:36:01.449848 IP h100n5c1o1031.bredband.skanova.com.3389 > Alpha.3143: P 10078:11476(1398) ack 875 win 64640 (DF)

[G] LICQ för Red Hat 8.0

Skicka meddelande:
20:23:22.631672 194.47.139.62.1042 > 64.12.30.208.5190: P 1242285186:1242285249(63) ack 26697832 win 8901 (DF)
20:23:22.946596 64.12.30.208.5190 > 194.47.139.62.1042: . ack 63 win 16384 (DF)

Skicka fil:
22:03:42.671783 194.47.139.63.3127 > 194.47.139.62.1052: S 1660275746:1660275746 (0) win 5840 <mss 1460,sackOK,timestamp 48694105 0,nop,wscale 0> (DF)
22:03:42.672001 194.47.139.62.1052 > 194.47.139.63.3127: S 3810351560:3810351560(0) ack 1660275747 win 5792 <mss 1460,sackOK,timestamp 1025698 48694105,nop,wscale 0> (DF)
22:03:42.672104 194.47.139.63.3127 > 194.47.139.62.1052: . ack 1 win 5840 <nop,nop,timestamp 48694106 1025698> (DF)
22:03:42.712690 194.47.139.63.3127 > 194.47.139.62.1052: P 1:3(2) ack 1 win 5840 <nop,nop,timestamp 48694126 1025698> (DF)

Ta emot fil:
Med Inbyggd brandvägg :
20:53:13.479701 h235n3c1o1031.bredband.skanova.com.3340 > 194.47.139.62.1067: S 2375333846:2375333846(0) win 65340 <mss 1452,nop,nop,sackOK> (DF)
20:53:13.479773 194.47.139.62 > h235n3c1o1031.bredband.skanova.com: icmp: 194.47.139.62 tcp port 1067 unreachable [tos 0xc0]
20:53:13.661552 h235n3c1o1031.bredband.skanova.com.3323 > 194.47.139.62.1040: . ack 69 win 65084 (DF)
20:53:16.398317 h235n3c1o1031.bredband.skanova.com.3340 > 194.47.139.62.1067: S 2375333846:2375333846(0) win 65340 <mss 1452,nop,nop,sackOK> (DF)
20:53:16.398385 194.47.139.62 > h235n3c1o1031.bredband.skanova.com: icmp: 194.47.139.62 tcp port 1067 unreachable [tos 0xc0]
20:53:22.412346 h235n3c1o1031.bredband.skanova.com.3340 > 194.47.139.62.1067: S 2375333846:2375333846(0) win 65340 <mss 1452,nop,nop,sackOK> (DF)
20:53:22.412416 194.47.139.62 > h235n3c1o1031.bredband.skanova.com: icmp: 194.47.139.62 tcp port 1067 unreachable [tos 0xc0]

[H] Windows Messenger för Windows XP

Skicka meddelande:
16:15:59.283184 IP Alpha.3525 > baym-sb10.msgr.hotmail.com.1863: P 804:971(167) ack 506 win 63346 (DF)
16:15:59.472716 IP baym-sb10.msgr.hotmail.com.1863 > Alpha.3525: . ack 971 win 1 7353

Skicka fil:
19:17:36.166164 IP Alpha.3642 > h29n3c1o1031.bredband.skanova.com.6891: S 396681908:396681908(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
19:17:36.192586 IP h29n3c1o1031.bredband.skanova.com.6891 > Alpha.3642: S 3798078131:3798078131(0) ack 396681909 win 65340 <mss 1452,nop,nop,sackOK> (DF)
19:17:36.192750 IP Alpha.3642 > h29n3c1o1031.bredband.skanova.com.6891: . ack 1win 65340 (DF)
19:17:36.193339 IP Alpha.3642 > h29n3c1o1031.bredband.skanova.com.6891: P 1:13(12) ack 1 win 65340 (DF)

Ta emot fil:
11:09:47.239473 IP Alpha.3959 > baym-sb6.msgr.hotmail.com.1863: S 407083880:407083880(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)

11:09:47.426882 IP baym-sb6.msgr.hotmail.com.1863 > Alpha.3959: S 1449430899:1449430899(0) ack 407083881 win 17520 <mss 1460,nop,nop,sackOK>
11:09:47.427044 IP Alpha.3959 > baym-sb6.msgr.hotmail.com.1863: . ack 1 win 64240 (DF)
11:09:47.427662 IP Alpha.3959 > baym-sb6.msgr.hotmail.com.1863: P 1:51(50) ack 1 win 64240 (DF)
11:09:47.433579 IP Alpha.3952 > baym-cs72.msgr.hotmail.com.1863: . ack 94 win 63264 (DF)

Chat
16:15:59.283184 IP Alpha.3525 > baym-sb10.msgr.hotmail.com.1863: P 804:971(167) ack 506 win 63346 (DF)
16:15:59.472716 IP baym-sb10.msgr.hotmail.com.1863 > Alpha.3525: . ack 971 win 1 7353

[I] Gaim för Red Hat 8.0

Skicka meddelande:
20:35:02.833545 194.47.139.62.1031 > 64.12.24.134.5190: P 2046558072:2046558144(72) ack 3282103896 win 10380 (DF)
20:35:02.956714 64.12.24.134.5190 > 194.47.139.62.1031: P 1:43(42) ack 72 win 16384 (DF)
20:35:02.956821 194.47.139.62.1031 > 64.12.24.134.5190: . ack 43 win 10380 (DF)

Chat
20:39:07.784181 caim-m01a.blue.aol.com.5190 > 194.47.139.62.1042: P 617:674(57) ack 1 win 16384 (DF)
20:39:07.784288 194.47.139.62.1042 > caim-m01a.blue.aol.com.5190: . ack 674 win 11700 (DF)
20:39:11.984043 caim-m01a.blue.aol.com.5190 > 194.47.139.62.1042: P 674:882(208) ack 1 win 16384 (DF)
20:39:11.984141 194.47.139.62.1042 > caim-m01a.blue.aol.com.5190: . ack 882 win 11700 (DF)

[J] Outlook för Windows XP

Skicka e-post:
19:45:17.744697 IP mothers.student.bth.se.25 > Alpha.3655: P 269:319(50) ack 91win 24820 (DF)
19:45:17.751784 IP Alpha.3655 > mothers.student.bth.se.25: P 91:1261(1170) ack 319 win 63922 (DF)
19:45:17.845304 IP mothers.student.bth.se.25 > Alpha.3655: . ack 1261 win 24820(DF)
19:45:17.845508 IP Alpha.3655 > mothers.student.bth.se.25: P 1261:1266(5) ack 319 win 63922 (DF)

Ta emot e-post:
19:44:51.753769 IP mothers.student.bth.se.110 > Alpha.3654: . 166:1626(1460) ack 50 win 24820 (DF)
19:44:51.753904 IP mothers.student.bth.se.110 > Alpha.3654: P 1626:2442(816) ack 50 win 24820 (DF)
19:44:51.754000 IP Alpha.3654 > mothers.student.bth.se.110: . ack 2442 win 64240 (DF)
19:44:51.973689 IP Alpha.3654 > mothers.student.bth.se.110: P 50:58(8) ack 2442 win 64240 (DF)

Nyhetsgrupper:
21:15:23.436791 IP Alpha.4616 > grc.com.119: . ack 71791 win 64240 (DF)
21:15:23.439848 IP grc.com.119 > Alpha.4616: . 74711:76171(1460) ack 60 win 17520 (DF)
21:15:23.439980 IP Alpha.4616 > grc.com.119: . ack 71791 win 64240 (DF)
21:15:23.453075 IP grc.com.119 > Alpha.4616: . 71791:73251(1460) ack 60 win 17520 (DF)

[K] Ximian för Red Hat 8.0

Skicka e-post:
21:15:51.317620 mothers.student.bth.se.smtp > 194.47.139.62.1082: P 347:399(52) ack 95 win 24616 <nop,nop,timestamp 1356647709 2987165> (DF)
21:15:51.320252 194.47.139.62.1082 > mothers.student.bth.se.smtp: P 95:101(6) ack 399 win 6432 <nop,nop,timestamp 2987173 1356647709> (DF)

Ta emot e-post:
21:05:55.900033 194.47.139.62.1071 > mothers.student.bth.se.pop3: S 1269947868:1269947868(0) win 5840 <mss 1460,sackOK,timestamp 2682318 0,nop,wscale 0> (DF)
21:05:55.900332 mothers.student.bth.se.pop3 > 194.47.139.62.1071: S 1500111432:1500111432(0) ack 1269947869 win 24616 <nop,nop,timestamp 1356588178 2682318,nop,wscale 0,nop,nop,sackOK,mss 1460> (DF)
21:05:55.900422 194.47.139.62.1071 > mothers.student.bth.se.pop3: . ack 1 win 5840 <nop,nop,timestamp 2682318 1356588178> (DF)
21:05:56.314170 mothers.student.bth.se.pop3 > 194.47.139.62.1071: P 1:38(37) ack 1 win 24616 <nop,nop,timestamp 1356588219 2682318> (DF)
21:05:56.314276 194.47.139.62.1071 > mothers.student.bth.se.pop3: . ack 38 win 5840 <nop,nop,timestamp 2682530 1356588219> (DF)

Nyhetsgrupper:
21:26:23.872674 grc.com.nntp > 194.47.139.62.1066: . 1517:2977(1460) ack 33 win 17520 (DF)
21:26:23.874978 grc.com.nntp > 194.47.139.62.1066: . 4437:5897(1460) ack 33 win 17520 (DF)
21:26:23.875035 194.47.139.62.1066 > grc.com.nntp: . ack 2977 win 62780 (DF)

[L] Webmail (IMAP) för Windows XP

Skicka e-post:
20:32:53.632783 IP Alpha.4367 > flygel.bth.se.443: S 1558173382:1558173382(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
20:32:53.633171 IP flygel.bth.se.443 > Alpha.4367: S 1956182035:1956182035(0) ack 1558173383 win 24820 <nop,nop,sackOK,mss 1460> (DF)

20:32:53.633270 IP Alpha.4367 > flygel.bth.se.443: . ack 1 win 64240 (DF)20:32:53.634715 IP Alpha.4367 > flygel.bth.se.443: P 1:103(102) ack 1 win 64240(DF)

Ta emot e-post:
15:01:07.485170 IP Alpha.3217 > flygel.bth.se.443: S 2685550644:2685550644(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
15:01:07.485670 IP flygel.bth.se.443 > Alpha.3217: S 3154857888:3154857888(0) ack 2685550645 win 24820 <nop,nop,sackOK,mss 1460> (DF)
15:01:07.485777 IP Alpha.3217 > flygel.bth.se.443: . ack 1 win 64240 (DF)
15:01:07.487486 IP Alpha.3216 > flygel.bth.se.443: P 103:170(67) ack 147 win 64094 (DF)

[M] Webmail (IMAP) för Red Hat 8.0

Skicka e-post:
22:41:02.050345 194.47.139.62.2184 > flygel.bth.se.https: P 2427:3377(950) ack 1015 win 7768 <nop,nop,timestamp 5603867 658549673> (DF)
22:41:02.157519 flygel.bth.se.https > 194.47.139.62.2184: . ack 3377 win 24616 <nop,nop,timestamp 658549684 5603867> (DF)
22:41:03.851801 flygel.bth.se.https > 194.47.139.62.2184: P 1015:2030(1015) ack 3377 win 24616 <nop,nop,timestamp 658549853 5603867> (DF)
22:41:03.890845 194.47.139.62.2184 > flygel.bth.se.https: . ack 2030 win 9135 <nop,nop,timestamp 5604810 658549853> (DF)

Ta emot e-post:
22:39:01.197840 flygel.bth.se.https > 194.47.139.62.2179: P 4323:4346(23) ack 998 win 24616 <nop,nop,timestamp 658537590 5541262> (DF)
22:39:01.222558 flygel.bth.se.https > 194.47.139.62.2179: . 4346:5794(1448) ack 998 win 24616 <nop,nop,timestamp 658537592 5541991> (DF)

[N] IRC för Windows XP

19:41:18.776493 IP efnet.demon.co.uk.6666 > Alpha.3651: P 3922729803:3922729940(137) ack 648734017 win 17520 (DF)
19:41:18.930720 IP Alpha.3651 > efnet.demon.co.uk.6666: . ack 137 win 63541 (DF)
19:41:20.011433 IP Alpha.3651 > efnet.demon.co.uk.6666: P 1:25(24) ack 137 win 63541 (DF)
19:41:20.159047 IP efnet.demon.co.uk.6666 > Alpha.3651: . ack 25 win 17496 (DF)
19:41:26.300740 IP Alpha.3651 > efnet.demon.co.uk.6666: P 25:63(38) ack 137 win 63541 (DF)
19:41:26.448753 IP efnet.demon.co.uk.6666 > Alpha.3651: . ack 63 win 17520 (DF)

[O] IRC för Red Hat 8.0

23:10:46.785153 194.47.139.62.2192 > efnet.demon.co.uk.ircd: P 530773502:530773528(26) ack 4174707500 win 43800 (DF)
23:10:46.925961 efnet.demon.co.uk.ircd > 194.47.139.62.2192: . ack 26 win 17520 (DF)
23:10:47.729025 194.47.139.62.2192 > efnet.demon.co.uk.ircd: P 26:48(22) ack 1 win 43800 (DF)
23:10:47.876150 efnet.demon.co.uk.ircd > 194.47.139.62.2192: . ack 48 win 17520 (DF)

[P] Sökningar för Windows XP

20:36:02.311880 IP Alpha.4385 > 216.239.57.99.80: P 1601513681:1601514116(435) ack 3568683373 win 64240 (DF)
20:36:02.511342 IP 216.239.57.99.80 > Alpha.4385: . ack 435 win 30660 (DF)
20:36:02.516692 IP 216.239.57.99.80 > Alpha.4385: P 93:178(85) ack 435 win 32120 (DF)
20:36:02.516797 IP Alpha.4385 > 216.239.57.99.80: . ack 1 win 64240 (DF)

[Q] Sökningar för Red Hat 8.0

21:44:04.465411 194.47.139.62.1117 > 216.239.51.99.http: S 3687997015:3687997015(0) win 5840 <mss 1460,sackOK,timestamp 3854064 0,nop,wscale 0> (DF)
21:44:04.588437 216.239.51.99.http > 194.47.139.62.1117: S 3500759792:3500759792(0) ack 3687997016 win 8190 <mss 1460>
21:44:04.588551 194.47.139.62.1117 > 216.239.51.99.http: . ack 1 win 5840 (DF)
21:44:04.589850 194.47.139.62.1117 > 216.239.51.99.http: P 1:623(622) ack 1 win 5840 (DF)
21:44:04.713920 216.239.51.99.http > 194.47.139.62.1117: . ack 623 win 30660 (DF) [tos 0x10]

[R] Spel för Windows XP

Warcraft III – ALPHA som server:
ICF logg:
2003-05-03 13:09:50 DROP UDP 62.20.240.220 194.47.142.15 6110 6112 44 - - - - - - -
2003-05-03 13:09:51 DROP UDP 62.20.240.220 194.47.142.15 6110 6112 44 - - - - - - -
2003-05-03 13:09:51 DROP UDP 62.20.240.220 194.47.142.15 6110 6112 44 - - - - - - -

windump:
13:12:23.749541 IP h220n7c1o1031.bredband.skanova.com.6110 > oblivion.rsn.bth.se.6112: udp 16
13:12:24.221234 IP h220n7c1o1031.bredband.skanova.com.6110 > oblivion.rsn.bth.se.6112: udp 16
13:12:24.721495 IP h220n7c1o1031.bredband.skanova.com.6110 > oblivion.rsn.bth.se.6112: udp 16

Warcraft III - ALPHA som klient:
ICF loggning klient:
2003-05-10 17:57:00 OPEN UDP 194.47.142.15 217.209.226.115 6110 6112 - - - - - - - -

2003-05-10 17:57:05 OPEN TCP 194.47.142.15 217.209.226.115 4381 6112 - - - - - - - -
2003-05-10 17:57:45 CLOSE TCP 194.47.142.15 217.209.226.115 4381 6112 - - - - - - - -
2003-05-10 17:58:45 CLOSE UDP 194.47.142.15 217.209.226.115 6110 6112 - - - - - - - -

windump:
17:57:00.461006 IP oblivion.rsn.bth.se.6110 > h115n5c1o1031.bredband.skanova.com.6112: udp 16
17:57:00.490971 IP h115n5c1o1031.bredband.skanova.com.6112 > oblivion.rsn.bth.se.6110: udp 124

17:57:05.000749 IP oblivion.rsn.bth.se.4381 > h115n5c1o1031.bredband.skanova.com
.6112: S 1736028894:1736028894(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)

[S] Mediaspelare för Windows XP

RealOne (svt´s portal)
21:36:27.575987 IP Alpha.4961 > 193.15.117.180.554: . ack 742786 win 64240 (DF)
21:36:27.576074 IP 193.15.117.180.554 > Alpha.4961: P 742786:743331(545) ack 1885 win 63909 (DF)
21:36:27.596427 IP 193.15.117.180.554 > Alpha.4961: P 743331:744791(1460) ack 1885 win 63909 (DF)
21:36:27.596681 IP Alpha.4961 > 193.15.117.180.554: . ack 744791 win 64240 (DF)

[T] Mediaspelare för Red Hat 8.0

22:14:27.826985 194.47.139.62.2153 > 193.15.117.180.rtsp: S 1322661132:1322661132(0) win 5840 <mss 1460,sackOK,timestamp 4787625 0,nop,wscale 0> (DF)
22:14:27.840576 193.15.117.180.rtsp > 194.47.139.62.2153: S 2778362701:2778362701(0) ack 1322661133 win 64240 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF)
22:14:27.840676 194.47.139.62.2153 > 193.15.117.180.rtsp: . ack 1 win 5840 <nop,nop,timestamp 4787632 0> (DF)
22:14:27.867957 194.47.139.62.2153 > 193.15.117.180.rtsp: P 1:403(402) ack 1 win 5840 <nop,nop,timestamp 4787646 0> (DF)

[U] Nedladdning för Windows XP

FTP
20:27:45.674270 IP Alpha.4350 > FTP1.21: S 1480591488:1480591488(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
20:27:45.785564 IP FTP1.21 > Alpha.4350: S 3093946239:3093946239(0) ack 1480591489 win 8760 <mss 1460> (DF)
20:27:45.785741 IP Alpha.4350 > FTP1.21: . ack 1 win 64240 (DF)
20:27:45.898855 IP FTP1.21 > Alpha.4350: P 1:60(59) ack 1 win 8760 (DF)
20:27:46.010974 IP Alpha.4350 > FTP1.21: . ack 60 win 64181 (DF)
20:27:46.122411 IP FTP1.21 > Alpha.4350: P 60:203(143) ack 1 win 8760 (DF)
20:27:46.136293 IP Alpha.4350 > FTP1.21: P 1:48(47) ack 203 win 64038 (DF)

HTTP
18:22:18.450207 IP 213.132.113.2.80 > Alpha.4272: . 13141:14601(1460) ack 278 win 6432 (DF)
18:22:18.450266 IP Alpha.4272 > 213.132.113.2.80: . ack 14601 win 58400 (DF)
18:22:18.460049 IP 213.132.113.2.80 > Alpha.4272: . 14601:16061(1460) ack 278 win 6432 (DF)

[V] Nedladdning för Red Hat 8.0

FTP
21:59:23.364762 ftp2.sunet.se.ftp > 194.47.139.62.1903: P 149:223(74) ack 1 win 33304 <nop,nop,timestamp 148928499 4324501>
21:59:23.364779 ftp2.sunet.se.ftp > 194.47.139.62.1903: P 223:297(74) ack 1 win 33304 <nop,nop,timestamp 148928499 4324501>

HTTP
21:53:59.137290 rockpile.student.bth.se.http > 194.47.139.62.1897: P 5024:6472(1448) ack 1054 win 24616 <nop,nop,timestamp 1356182230 4158519> (DF)
21:53:59.137320 194.47.139.62.1897 > rockpile.student.bth.se.http: . ack 6472 win 18824 <nop,nop,timestamp 4158536 1356182230> (DF)
21:53:59.137426 rockpile.student.bth.se.http > 194.47.139.62.1897: P 6472:7920(1448) ack 1054 win 24616 <nop,nop,timestamp 1356182230 4158519> (DF)

[W] Köp & Sälj för Windows XP

Internet Bank
19:15:01.026840 IP Alpha.4493 > swp2.vv.sebank.se.443: S 661143072:661143072(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
19:15:01.042860 IP swp2.vv.sebank.se.443 > Alpha.4493: S 2282698340:2282698340(0) ack 661143073 win 32768 <mss 1460,nop,nop,sackOK> (DF)
19:15:01.043071 IP Alpha.4493 > swp2.vv.sebank.se.443: . ack 1 win 64240 (DF)

Beställning av vara (köpet slutfördes)
20:09:13.815543 194.47.139.62.1082 > 194.68.214.178.https: S 1514547434:1514547434(0) win 5840 <mss 1460,sackOK,timestamp 305064 0,nop,wscale 0> (DF)
20:09:13.828631 194.68.214.178.https > 194.47.139.62.1082: S 1271593164:1271593164(0) ack 1514547435 win 65160 <nop,nop,timestamp 222526132 305064,nop,wscale 0,mss 1460> (DF)
20:09:13.828772 194.47.139.62.1082 > 194.68.214.178.https: . ack 1 win 5840 <nop,nop,timestamp 305071 222526132> (DF)
20:09:13.829644 194.47.139.62.1082 > 194.68.214.178.https: P 1:73(72) ack 1 win 5840 <nop,nop,timestamp 305071 222526132> (DF)

[X] Köp & Sälj för Red Hat 8.0

Internet bank
12:43:50.930944 194.47.139.62.3404 > swp2.vv.sebank.se.https: S 2639683815:2639683815(0) win 5840 <mss 1460,sackOK,timestamp 1199687340,nop,wscale 0> (DF)
12:43:50.944114 swp2.vv.sebank.se.https > 194.47.139.62.3404: S 1986153184:1986153184(0) ack 2639683816 win 32768 <mss 1460,nop,nop,sackOK,wscale 0,nop,nop,nop,timestamp 1485989433 119968734> (DF)
12:43:50.944238 194.47.139.62.3404 > swp2.vv.sebank.se.https: . ack 1 win 5840 <nop,nop,timestamp 119968741 1485989433> (DF)
12:43:50.945158 194.47.139.62.3404 > swp2.vv.sebank.se.https: P 1:99(98) ack 1 win 5840 <nop,nop,timestamp 119968741 1485989433> (DF)
12:43:50.971280 swp2.vv.sebank.se.https > 194.47.139.62.3404: P 1:147(146) ack 99 win 32768 <nop,nop,timestamp 1485989436 119968741> (DF)

Beställning av vara (köpet slutfördes):
20:58:06.538487 194.47.139.62.2934 > www.sf.se.https: S 1798246445:1798246445(0) win 5840 <mss 1ckOK,timestamp 46678805 0,nop,wscale 0> (DF)
20:58:06.548204 www.sf.se.https > 194.47.139.62.2934: S 162158688:162158688(0) ack 1798246446 wi5 <mss 512>
20:58:06.548327 194.47.139.62.2934 > www.sf.se.https: . ack 1 win 5840 (DF)
20:58:06.549334 194.47.139.62.2934 > www.sf.se.https: P 1:99(98) ack 1 win 5840 (DF)
20:58:06.559339 www.sf.se.https > 194.47.139.62.2934: P 1:80(79) ack 99 win 65535

Brandväggarnas agerande / regler:

[aa] Iptables regler för Security Level Configuration Tool (SLCT) högsta säkerhet:

Chain INPUT (policy ACCEPT)

Target	prot	opt	source	destination
RH-Lokkit-0-50-INPUT	all	--	anywhere	anywhere

Chain FORWARD (policy ACCEPT)

Target	prot	opt	source	destination
RH-Lokkit-0-50-INPUT	all	--	anywhere	anywhere

Chain OUTPUT (policy ACCEPT)

Target	prot	opt	source	destination

Chain RH-Lokkit-0-50-INPUT (2 references)

Target	prot	opt	source	destination	
ACCEPT	all	--	anywhere	anywhere	
ACCEPT	udp	--	cymbal.bth.se	anywhere	udp spt:domain
REJECT	tcp	--	anywhere	anywhere	tcp flags:SYN,RST,ACK/SYN reject-with icmp-port-unreachable
REJECT	udp	--	anywhere	anywhere	udp reject-with icmp-port-unreachable

[ab] Iptables regler för Security Level Configuration Tool – avstängd:

Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

[ac] ICF agerande:

2003-05-02 16:29:36 OPEN UDP 194.47.139.62 194.47.139.1 3009 1900 - - - - - - - -
2003-05-05 13:19:56 CLOSE UDP 194.47.139.62 194.47.139.1 3009 1900 - - - - - - - -

2003-05-05 13:25:33 OPEN UDP 194.47.139.62 194.47.129.10 1026 53 - - - - - - - -
2003-05-05 13:26:56 CLOSE UDP 194.47.139.62 194.47.129.10 1026 53 - - - - - - - -

2003-05-07 12:56:25 DROP TCP 194.47.139.63 194.47.139.62 59415 31561 60 S 3389835588 0 2048 - - -
2003-05-07 12:56:25 DROP TCP 194.47.139.63 194.47.139.62 59416 31561 60 A 3389835588 0 2048 - - -
2003-05-07 12:56:25 DROP TCP 194.47.139.63 194.47.139.62 59417 31561 60 FUP 3389835588 0 4096 - - -

SCB:

[ae] SCBs undersökning fråga 7

Kommunikation 58,5 %
Informationssökning 67,4 %
Köp och försäljning 47,4 %
Myndighetskontakt 42,0 %

C. Syftet med användning av Internet
7 (C1) För vilket eller vilka av följande privata syften har Du använt Internet under tiden januari t.o.m. mars
svarsalternativ ja/nej
a) skicka och ta emot e-post
b) Internettelefoni
c) videokonferens
d) chatta
e) söka information om varor och tjänster
f) använda tjänster med anknytning till resor och inkvartering
g) distansutbildning
h) använda tjänster med anknytning till hälsa och sjukvård
i) lyssna på radio (webbradio)
j) titta på TV (webb-TV)
k) lyssna till musik
l) ”ladda ner” musik
m) spela spel
n) ladda ner spel
o) läsa nättidningar eller elektroniska tidskrifter
p) finansiella tjänster, t.ex. bankärenden eller köp av aktier
q) köp eller beställning av varor och tjänster (utom aktier eller finansiella tjänster)
r) försäljning av varor och tjänster
s) hämta information från myndigheters hemsidor
t) ”ladda ner” myndigheters formulär eller blanketter
u) skicka ifyllda formulär eller blanketter till myndigheter
v) leta efter nytt arbete eller skicka arbetsansökningar

Versions nummer applikationerna:

[af] Applikationsversioner som används under funktionalitetstestet för Windows XP

Tjänst	Applikation	Version
IM	ICQ	2003a
IM	Windows Messenger	4.6
E-post	Outlook Express	6
Nyhetsgrupper	Outlook Express	6
Webmail	IMP	2.2.6
IRC	mIRC	6.03
Spel	Warcraft III	1.05
Mediaspelare	Real One	2.0
Nedladdning	Cute FTP Pro	1.0
	Internet Explorer	6.0

[ag] Applikationsversioner som används under funktionalitetstestet för Red Hat Linux 8.0

Tjänst	Applikation	Version
IM	LICQ	1.2.0
IM	Gaim	0.59.1
E-post	Ximian	1.0.8
Nyhetsgrupper	Knode	0.7.1
Webmail	IMP	2.2.6
IRC	X-Chat	1.8.10
Spel	-	-
Mediaspelare	Real Audio	8
Nedladdning	gFTP	2.0.13
	Mozilla	1.0.1