ÖVERGÅNGEN TILL IPV6: SÄKERHETSRISKER

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2012

Marcus Karlsson

Handledare: Birgitta Lindström
Examinator: Henrik Gustavsson
Sammanfattning


Nyckelord: Säkerhetsrisker, IPv6, Systemadministratörer, Medvetenhet, Övergång
# Innehållsförteckning

<table>
<thead>
<tr>
<th>1</th>
<th>Introduktion</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Bakgrund</td>
<td>2</td>
</tr>
<tr>
<td>2.1</td>
<td>Datakommunikation</td>
<td>2</td>
</tr>
<tr>
<td>2.2</td>
<td>TCP/IP</td>
<td>2</td>
</tr>
<tr>
<td>2.3</td>
<td>IPv4</td>
<td>2</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Reserverade adresser</td>
<td>3</td>
</tr>
<tr>
<td>2.3.2</td>
<td>NAT</td>
<td>4</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Fragmentering</td>
<td>4</td>
</tr>
<tr>
<td>2.3.4</td>
<td>ICMP</td>
<td>4</td>
</tr>
<tr>
<td>2.3.5</td>
<td>Header</td>
<td>4</td>
</tr>
<tr>
<td>2.4</td>
<td>IPv6</td>
<td>4</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Header</td>
<td>5</td>
</tr>
<tr>
<td>2.4.2</td>
<td>Adressklasser</td>
<td>5</td>
</tr>
<tr>
<td>2.4.3</td>
<td>IPsec</td>
<td>6</td>
</tr>
<tr>
<td>2.4.4</td>
<td>Autokonfiguration</td>
<td>6</td>
</tr>
<tr>
<td>2.4.5</td>
<td>NDP</td>
<td>6</td>
</tr>
<tr>
<td>2.4.6</td>
<td>Extension headers</td>
<td>6</td>
</tr>
<tr>
<td>2.5</td>
<td>Övergångsmekanismer</td>
<td>7</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Tunneling</td>
<td>7</td>
</tr>
<tr>
<td>2.5.2</td>
<td>Dual-stack</td>
<td>7</td>
</tr>
<tr>
<td>2.6</td>
<td>Informationssäkerhet och säkerhetsrisker</td>
<td>7</td>
</tr>
<tr>
<td>2.7</td>
<td>Relaterade arbeten</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Problem</td>
<td>9</td>
</tr>
<tr>
<td>3.1</td>
<td>Problemprecisering</td>
<td>9</td>
</tr>
<tr>
<td>3.2</td>
<td>Delmål</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>Metod och genomförande</td>
<td>11</td>
</tr>
<tr>
<td>4.1</td>
<td>Metod</td>
<td>11</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Delmål 1</td>
<td>11</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Delmål 2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.3</td>
<td>Delmål 3</td>
<td>12</td>
</tr>
<tr>
<td>4.2</td>
<td>Genomförande</td>
<td>12</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Delmål 1</td>
<td>12</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Delmål 2</td>
<td>12</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Delmål 3</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>Resultat och analys</td>
<td>14</td>
</tr>
<tr>
<td>5.1</td>
<td>Säkerhetsrisker</td>
<td>14</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Routing header</td>
<td>14</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Fragmentering</td>
<td>14</td>
</tr>
<tr>
<td>5.1.3</td>
<td>ICMPv6</td>
<td>14</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Duplicate Address Detection</td>
<td>14</td>
</tr>
<tr>
<td>5.1.5</td>
<td>Granncache</td>
<td>15</td>
</tr>
<tr>
<td>5.1.6</td>
<td>Neighbor Unreachability Detection</td>
<td>15</td>
</tr>
<tr>
<td>5.1.7</td>
<td>Standardroutern</td>
<td>15</td>
</tr>
<tr>
<td>5.1.8</td>
<td>Adresser för ett givet prefix</td>
<td>15</td>
</tr>
</tbody>
</table>
5.1.9 Hop-by-hop options header .............................................................15
5.1.10 Felaktigt prefix i det lokala nätverket .........................................16
5.1.11 Tunningsmekanismer ..................................................................16
5.1.12 Autokonfiguration ......................................................................16
5.2 Webbenkät .......................................................................................16
5.2.1 Deltagarna i enkäten .....................................................................17
5.2.2 Medvetenhet om risker med routing header ....................................17
5.2.3 Medvetenhet om risk med fragmentering .......................................18
5.2.4 Medvetenhet om risk med Duplicate address detection ....................19
5.2.5 Medvetenhet om risk med standardroutern ....................................20
5.2.6 Medvetenhet om risk med Hop-by-hop options header ....................20
5.2.7 Medvetenhet om risk med granncache ...........................................21
5.2.8 Medvetenhet om risk med tunningsmekanismer ..............................22
5.2.9 Medvetenhet om risk med autokonfiguration ..................................23
5.2.10 Medvetenhet om risk med felaktigt prefix i det lokala nätverket .......24
5.2.11 Medvetenhet om risk med adresser för ett givet prefix ....................24
5.2.12 Medvetenhet om risk med ICMPv6 ...............................................25
5.2.13 Sammanfattande analys ...............................................................26
6 Slutsats och diskussion ......................................................................29
6.1 Slutsats ............................................................................................29
6.2 Diskussion .......................................................................................30
6.3 Framtida arbete .................................................................................32

Bilaga A Inbjudan till enkät

Bilaga B Enkäten
1 Introduktion

Sammankopplade datorer, skrivare och liknande enheter som sänder data till varandra med hjälp av ett protokoll (styr hur enheterna ska kommunicera) kallas för ett datanätverk. I de flesta moderna datanätverk använder alla enheter protokollet, Internet Protocol (IP), vilket möjliggör att det bland annat går att sända och ta emot information över nätverk. För närvarande används mestadels version fyra av detta protokoll (IPv4). För att unikt identifiera de olika enheterna, även kallade noderna, i ett nätverk ges de en adress, en så kallad IPv4-adress.


Datorer används för allt från att utföra bankärende till att kommunicera med andra över mail. Denna information bör oftast inte kunna läsas av obehöriga, särskilt kontouppgifter och dylikt, vilket gör att säkerheten anses väldigt viktig i datornätverk.

Syftet med detta arbete är att undersöka vilka säkerhetsrisker som finns vid en övergång från IPv4 till IPv6 och vilken medvetenhet systemadministratörer har om dessa.
2 Bakgrund


2.1 Datakommunikation


2.2 TCP/IP


2.3 IPv4


Tekniker som NAT (Network Address Translation) och CIDR (Classless Inter-Domain Routing) har gjort att IPv4 fortfarande används i en bred skala idag. IPv4 adresser
representeras på särskilt sätt kallat Dot-decimal notation, vilket innebär att de innehåller strängar av siffror som separeras med punkter. Till exempel 123.6.56.1 som är en giltig IP-adress (Postel & Vernon, 1983).

Detta delkapitel beskriver de adresser som är reserverade vid användning av IPv4-protokollet. Vidare diskuteras IPv4-header, fragmentering, Internet Control Message Protocol och NAT.

2.3.1 Reserverade adresser
I praktiken finns inte 4 294 967 296 att tillgå då flera adresser är reserverade för andra särskilda ändamål. Dessa finns att se nedan i Tabell 1 (Cotton & Vegoda, 2010).

<table>
<thead>
<tr>
<th>Adressspann</th>
<th>Andamål</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0–0.255.255.255</td>
<td>Broadcast (skicka data till alla enheter i nätverket) till nuvarande nätverk</td>
</tr>
<tr>
<td>10.0.0.0–10.255.255.255</td>
<td>Privata nätverk</td>
</tr>
<tr>
<td>127.0.0.0–127.255.255.255</td>
<td>Loopback</td>
</tr>
<tr>
<td>169.254.0.0–169.254.255.25</td>
<td>Autokonfiguration</td>
</tr>
<tr>
<td>172.16.0.0–172.31.255.255</td>
<td>Privata nätverk</td>
</tr>
<tr>
<td>192.0.2.0–192.0.2.255</td>
<td>Benämns TEST-NET 1 och används för dokumentation och exempelkod</td>
</tr>
<tr>
<td>192.88.99.0–192.88.99.255</td>
<td>IPv6 till IPv4 relay</td>
</tr>
<tr>
<td>192.88.99.0–192.88.99.255</td>
<td>IPv6 till IPv4 relay</td>
</tr>
<tr>
<td>192.168.0.0–192.168.255.255</td>
<td>Privata nätverk</td>
</tr>
<tr>
<td>198.18.0.0–198.19.255.255</td>
<td>Nätverksbenchmark</td>
</tr>
<tr>
<td>198.51.100.0–198.51.100.255</td>
<td>Benämns TEST-NET 2 och används för dokumentation och exempelkod</td>
</tr>
<tr>
<td>203.0.113.0–203.0.113.255</td>
<td>Benämns TEST-NET 3 och används för dokumentation och exempelkod</td>
</tr>
<tr>
<td>224.0.0.0–239.255.255.255</td>
<td>Multicast (skicka data till en grupp av alla enheter i nätverket)</td>
</tr>
<tr>
<td>240.0.0.0–255.255.255.255</td>
<td>255.255.255.255 används för broadcast och övriga adresser är reserverade för framtida allokering</td>
</tr>
</tbody>
</table>
2.3.2 NAT
NAT är en av de tekniker som dämpat bristen på IP-adresser. NAT sparar adresser då endast en eller ett fåtal adresser används för ett lokalt nätverk bestående av flertalet datorer när de skall kommunicera med andra enheter ute på Internet. När enheter kommunicerar lokalt med varandra används dock varsin unik privat adress (Halsall, 2005). Dessa block av privata adresser finns att se i Tabell 1.

2.3.3 Fragmentering
När ett paket som har en större storlek än destinationens, ett mellanliggande nätverks eller en routers MTU (Maximum Transmission Unit), den största paketstorleken som stöds, anländer måste detta delas upp i mindre delar, så kallade fragment. Det är sedan mottagarens uppgift att sammanfoga paketet igen med hjälp av information i fragmenten (Halsall, 2005).

2.3.4 ICMP
Internet Control Message Protocol (ICMP) är en viktig del av IP-protokollet. ICMP används av routrar, datorer och andra enheter för att till exempel svara på fel i IP-paket, diagnostisering eller i routingsyften. Ett vanligt nätverksverktyg som använder ICMP är Ping där det undersöks huruvida en enhet är kontaktbar eller inte (Halsall, 2005).

2.3.5 Header
Ett IPv4-paket består av en header och payload. Payload är den data som skall skickas medan headern till exempel innehåller adress- och kontrollfält. Headern för IPv4 finns att se nedan i Figur 1. Denna header består av treton fält som tolkas av routrar, datorer och andra enheter när de erhåller paket (Halsall, 2005).

![IPv4-header](https://example.com/rf791)

**Figur 1** IPv4-header (RFC 791)

2.4 IPv6


### 2.4.1 Header

Headern i IPv6 skiljer sig på flera ställen jämfört med sin föregångare. Antalet fält har minskats från tretton till åtta (se Figur 2), för att routrar skall kunna processa paket snabbare. Headern är i det stora hela enklare och mer effektiv (Deering & Hinden, 1998).

![IPv6-header](Deering & Hinden, 1998)

### 2.4.2 Adresskategorier

Det finns tre olika typer av adresser (Deering & Hinden, 1998):


- **Anycast** – Identifierar en grupp av gränssnitt som vanligtvis tillhör flera olika enheter. Ett paket som skickas till en anycast-adress levereras till det närmaste gränssnittet.

- **Multicast** – Identifierar en grupp av gränssnitt som vanligtvis tillhör flera olika enheter. Ett paket som skickas till en multicast-adress levereras till alla gränssnitt som ingår i gruppen.
2.4.3 IPsec

AH används för att autentisera paket och säkerhetsställa att paket inte har ändrats under transport. Det syftar till att skydda mot otillåten modifiering av IP-paket och förfalskning av paket. ESP förser IP-paketet med ytterligare inkapsling som innehåller kryptering för att inga obehöriga skall kunna läsa paketets innehåll. ESP kan också uppfylla AH:s funktioner, det vill säga autentisering och så vidare.

Både ESP och AH använder sig av tekniken SA (Security Association) för att mottagare och sändare skall komma överens om säkerhetsalgoritmer och andra parametrar. En IPv6-enhet har en mängd etablerade SA:s för varje säker kommunikationskanal som är aktiv (Kent, BBN Corp & Atkinson, 1998).

2.4.4 Autokonfiguration

2.4.5 NDP


- Router Advertisement (RA)-meddelanden skickas av routrar för att meddela att de finns tillgängliga. Dessa meddelanden sänds periodvis.
- Router Solicitation (RS) skickas av enheter för att begära att routrar skickar RA:s.
- Neighbor Solicitation (NS)-meddelanden används för att begära information om en annan enhets MAC (Medium Access Control)-adress, men också för till exempel upptäckt av adresskonflikt.
- Neighbor Advertisement (NA)-meddelandena svarar på NS-meddelanden, men kan även skickas av enheter som byter MAC-adress.

2.4.6 Extension headers
Extension headers används för att de flesta paketen inte innehåller någon extra avancerad information. De grundläggande fälten i IPv6-headern räcker oftast till. Ibland uppkommer dock situationer där det inte gör det och då används extension headers. Extension headers placeras mellan IPv6-headern och det övre lagrets header. Next header-fältet (se Figur 2)
används för att ange att fler headers följer. Exempel på extension headers är: routing, ESP och AH (Halsall, 2005).

2.5 Övergångsmekanismer


2.5.1 Tunneling

Tunneling gör det möjligt att skicka IPv6-trafik över den nuvarande IPv4-infrastrukturen i tunnlar. IPv6-paketen kapslas helt enkelt in i IPv4-paket och "tunnlas" över nätverket (Giligan, FreeGate Corp., Nordmark & Sun Microsystems, Inc, 2000).

2.5.2 Dual-stack


2.6 Informationssäkerhet och säkerhetsrisker

För att förstå säkerheten i nätverk finns tre aspekter, vilka är grundstenarna inom informationssäkerhet, som bör beaktas för att kunna skydda information från obehöriga (Pfleeger & Pfleeger, 2003):

- Konfidentialitet – säkerhetsställer att endast de personer som bör ha tillgång till information får tillgång till den.
- Integritet – syftar till att endast behöriga skall kunna modifiera information.
- Tillgänglighet – innebär att auktoriserade personer vid rätt tillfälle skall kunna komma åt information.


Detta examensarbete kommer att fokusera på kommunikationssäkerhet och säkerhetsrisker som bryter mot tillgänglighetsegenskapen. Kommunikationssäkerhet syftar till att skydda nätverk och andra medium som förmedlar information mellan datorer (Åhlfeldt, Spagnoletti & Sindre, 2007).

2.7 Relaterade arbeten


Hou, Zhao & Ma (2010) diskuterar i sin artikel bland annat grundläggande information om övergångsmechanismer och föreslår en lösning på en smidig övergång till IPv6 som baseras på tunneling och översättning. Tre olika faser beskrivs där olika övergångstekniker används i olika faser.

Inget vetenskapligt material som diskuterar vilken medvetenhet av säkerhetsrisker kring tillgänglighet som finns hos systemadministratörer vid en övergång från IPv4 till IPv6 har påträffats.
3 Problem


En framtidiga övergång till IPv6 är oundviklig, då IP-adresserna mer eller mindre är slut, samtidigt som det gamla IPv4-protokollet inte längre håller mättet bland annat på grund av säkerhetsproblem.


Denna rapport kommer att fokusera på att undersöka vilka säkerhetsrisker som finns gällande tillgänglighet vid en övergång från IPv4 till IPv6 och vilken medvetenhet systemadministratörer har om dessa risker. Rapporten kan användas som ett underlag för organisationer så att de kan vara mer förberedda på hur de skall skydda sig emot framtida skada, eftersom rapporten sammanställer vilka säkerhetsrisker som finns och insikt i hur medvetna systemadministratörer är i denna fråga. Därmed kan behovet av lämplig utbildning identifieras så att organisationer kan förbereda sig på att reagera snabbt när nya svagheter upptäcks.

3.1 Problemprecisering

Problemet är osäkerheten kring den förändrade riskbilden hos systemadministratörer vid övergången till IPv6. För att adressera problemet så syftar detta arbete till att besvara följande frågeställning:

- Vilka säkerhetsrisker gällande tillgänglighet finns vid en övergång från IPv4 till IPv6 och vilken medvetenhet om dessa har systemadministratörer?

3.2 Delmål

För att på ett enklare sätt kunna behandla problemet har tre delmål framtagits:
**Delmål 1:** Identifiera och sammanställa de olika säkerhetsriskerna gällande tillgänglighet som finns vid en övergång till IPv6.

**Delmål 2:** Undersöka systemadministratörers medvetenhet om de säkerhetsrisker gällande tillgänglighet som uppkommer vid en övergång till IPv6.

**Delmål 3:** Jämföra och sammanställa resultaten från de föregående delmålen och dra slutsatser utifrån dessa.
4 Metod och genomförande

I detta kapitel presenteras de valda metoderna, för- och nackdelar diskuteras med de olika lämpliga metoderna och slutligen beskrivs hur arbetet genomfördes.

4.1 Metod

Detta delkapitel beskriver möjliga metoder och dess för- och nackdelar för respektive delmål i arbetet.

4.1.1 Delmål 1


4.1.2 Delmål 2

När systemadministratörers medvetenhet om de säkerhetsrisker gällande tillgänglighet som uppkommer vid en övergång till IPv6 skall undersökas kommer en enkät att genomföras. Fördelen med att utföra en enkät är att det är möjligt med relativt få resurser erhålla svar från många respondenter (Berndtsson, et al., 2002), eftersom tiden för detta examensarbete är begränsad samtidigt som det är ett enmansjobb anses denna metod vara mest lämpad i förhållande till de resurser som finns att tillgå. Även om svarsfrekvensen inte blir hög är fortfarande enkäten och dess genomförande ett bidrag som kan redovisas i resultatet. En enkät ger dock inget utrymme för synkron kommunikation, vilket gör det omöjligt att ge ytterligare förklaringar på frågor som upplevs svåra att besvara. En annan nackdel med att utföra en enkät är att motivationen för deltagande ofta är låg (Berndtsson, et al., 2002).


Ett annat alternativ till enkät skulle vara intervju där frågor skulle ställas till systemadministratörer för att undersöka deras medvetenhet. Denna metod valdes inte av anledningen att med den tid som finns tillgänglig skulle endast ett fåtal
systemadministratörer kunna intervjuas och detta skulle kanske ge en felaktig bild, eftersom så få deltagare skulle inkluderas. Det skulle bli svårt att få en helhetsbild.

4.1.3 Delmål 3
Slutligen kommer en jämförande analys av resultaten från litteraturstudien och webbenkätna att genomföras i syfte att fastställa medvetenheten hos systemadministratörer om de säkerhetsrisker gällande tillgänglichkeit som uppkommer vid en övergång till IPv6.

4.2 Genomförande
I detta delkapitel presenteras genomförandet för varje delmål i rapporten.

4.2.1 Delmål 1

4.2.2 Delmål 2

Inledningen i webbenkäten syftar till att ge en kort introduktion till de tre delarna. Vidare betonas att det är viktigt att respondenten inte tar hjälp av andra källor, eftersom det skulle ge en felaktig bild av systemadministratörernas medvetenhet.


Den andra delen av webbenkäten innehåller frågor om de säkerhetsrisker som har framtagits. Eftersom frågor om viss säkerhetsrisk följer en fråga som syftar till att undersöka hur säker respondenten är på sitt svar. Detta på grund av att undersöka om systemadministratörerna tror att de har mer kunskap än vad de egentliga har eller tvärtom.
Den tredje delen i enkäten innehåller en fråga som låter respondenten uttrycka sina tankar om enkäten till exempel reflektioner, funderingar, kritik eller något övrigt som respondenten önskar tillägga.


4.2.3 Delmål 3
5 Resultat och analys

Detta kapitel beskriver inledningsvis de olika säkerhetsriskerna som framtagits med hjälp av litteraturstudien. Därefter framställs och analyseras svaren från webbenkäten. Slutfilen presenteras en sammanfattande och djupare analys av systemadministratörernas medvetenhet.

5.1 Säkerhetsrisker

Detta delkapitel presenterar de säkerhetsrisker som identifierades genom en litteraturstudie. Totalt har tolv olika säkerhetsrisker sammanställt.

5.1.1 Routing header


5.1.2 Fragmentering

Enligt IPv6-specifikationen får inte noder mellan mottagare och sändare fragmentera paket. Genom att använda fragmentering kan en angripare få det första fragment att sakna portnummer och på så sätt kan accesskontroller som filtrerar på portnummer undvikas (om de inte sammanfogar alla fragment först). En angripare kan sända många små fragment och eventuellt få ett offers system att krascha, eftersom den buffer som skall sammanfoga alla fragment inte kan hantera den stora mängd fragment en angripare skickar. Systemet kan då alltså bli överbelastat och den normala användningen av systemet hindras i så fall (Chasser, 2010; Durdagi & Buldu, 2010; Zagar, Grgic & Rimac-Drlje, 2007).

5.1.3 ICMPv6


5.1.4 Duplicate Address Detection

Angripare kan genom att förfalska Neighbor Advertisements få DAD (Duplicate Address Detection) processen att misslyckas för en värd som försöker erhålla en IP-adress med hjälp av autokonfiguration. Värden kommer då sluta att förorsöka erhålla den adressen. Det kan bli

5.1.5 Granncache

5.1.6 Neighbor Unreachability Detection

5.1.7 Standardroutern
Standardroutern kan göras onåbar genom att duplicera Router Advertisements med parametern router lifetime satt till 0, då kommer värdena i nätverket tro att det inte finns någon standard router och då nekas de tillgång till Internet (Beck, Cholez, Festor & Chrisment, 2007; Choudhary, 2009).

5.1.8 Adresser för ett givet prefix

5.1.9 Hop-by-hop options header
5.1.10 Felaktigt prefix i det lokala nätverket
En angripare kan skicka ett förfalskat Router Advertisement-meddelande som anger att ett prefix finns i det lokala nätverket. Om en värd tror att ett prefix finns lokalt kommer den aldrig att skicka paket med det prefixet till routern. Istället kommer värden att försöka utföra adress resolution genom att skicka Neighbor Solicitations, men värden kommer aldrig att få några svar på dessa och nekas kommunikation med det prefix som angavs i det förfalskade Router Advertisement-meddelandet (Beck, Cholez, Festor & Chrisment, 2007; Arkko, Mäntylä, Aura, Nikander, Kempf & Roe, 2002; Choudhary, 2009; Caicedo, Joshi & Tuladhar, 2009).

5.1.11 Tunnlingsmekanismer
Tunnlingsmekanismer kan medföra att det blir enklare för en angripare att undvika filtrering för inkommande paket. Det är särskilt viktigt att övervaka automatiska tunnlingsmekanismer. Det finns två typer av metoder för automatisk tunnling. Den första kallas 6to4 och denna kapslar in IPv6-paket direkt i IPv4-paketet. Den andra mekanismen kallas teredo och innebär att IPv6-paket inkapslas i IPv4-UDP-paket. Om dessa två tunnlingsmekanismer används måste noder som mottar paket tillåta att paket från alla källadresser dekapsuleras. Detta kan innebära stora säkerhetsrisker. 6to4-arkitekturen inkluderar 6to4-routrar och 6to4-relay routrar. 6to4-routrar tar emot och dekapsulerar paket från andra 6to4-routrar och 6to4-relay routrar tar emot och dekapsulerar paket från noder som bara använder IPv6. IP-adresser i IPv4-headers respektive IPv6-headers kan förfalskas, vilket innebär att denna mekanism kan utnyttjas för att utföra DoS-attacker. Detta eftersom paket hela tiden kan skickas från olika källadresser, vilket gör det omöjligt för exempelvis en brandvägg att särskilja DoS-trafik från vanlig legitim trafik (Zagar, Grgic & Rimac-Drlje, 2007; Choudhary, 2009; Szigeti & Risztics, 2004).

5.1.12 Autokonfiguration

5.2 Webbenkät
Totalt har 10 av de 90 tillfrågade personer valt att delta i enkäten. Svarsfrekvensen är alltså cirka 11 procent. Fastän påminnelser i form av mail har skickats ut har en klar majoritet valt att inte genomföra enkäten. En respondent från en högskola har också angett att de inte önskar delta i undersökningen med motiveringen: ”Vi har hittills vägrat att implementera IPv6 beroende på att protokollet är bedrövligt och ogenomtänkt. Så frågorna är inte relevanta för vår del.” Hur den låga svarsfrekvensen påverkar tillförlitligheten för de slutsatser som dras med hänsyn till de erhållna enkätsvaren diskuteras i kapitel 6. Detta delkapitel presenterar de svar som har erhållits.
5.2.1 Deltagarna i enkäten

Figur 4 Utbildningsnivå

Av de tio personer som har besvarat enkäten så har majoriteten (se Figur 4) en eftergymnasial utbildning som är kortare än tre år. Generellt har de flesta deltagarna en relativt hög utbildningsnivå, då 70 % har fortsatt att studera efter gymnasiet.

Figur 5 Erfarenhet av IPv6

Endast 20 % av de personer som har besvarat enkäten har erfarenhet av att administrera IPv6, vilket indikerar att IPv6 fortfarande inte används i någon större utsträckning. Detta kan utläsas av Figur 5 ovan.

5.2.2 Medvetenhet om risker med routing header
30 % av de (se Figur 6) som har besvarat enkäten har angivit ett korrekt svar (Routing) på frågan ” Vilken IPv6 Extension Header kan av en angripare utnyttjas för att undvika accesskontroller som filtrerar på destinationsadress?” Nio av tio gissade också på denna fråga. Detta tyder på en omedvetenhet om denna risk samtidigt som majoriteten av deltagarna inte heller tror att de har kunskap om risken.
Figur 6 Risk med routing header

På frågan "Vilken IPv6 Extension Header kan av en angripare utnyttjas för att undvika accesskontroller som filtrerar på destinationsadress?" har endast en av tio respondenter (se Figur 7 nedan) angett rätt svar (Routing), vilket tyder på en väldigt låg medvetenhet om denna risk. Även här anger de flesta dock att de är väldigt osäkra på sitt svar.

Figur 7 Risk med routing header

5.2.3 Medvetenhet om risk med fragmentering
20 % av deltagarna (se Figur 8) i enkäten har angett det rätta svaret (Skicka fragmenterade paket där det första fragmentet saknar portnummer (paketet sammansätts inte av mottagande enhet)) på frågan "Med vilken av följande metoder kan en angripare undvika accesskontroller?" Detta indikerar en låg medvetenhet och samtliga deltagare har valt att ange att de har gissat på frågan, vilket ytterligare stärker det föregående påståendet.
5.2.4 Medvetenhet om risk med Duplicate address detection

Endast 10% av respondenterna (se Figur 9) har angett rätt svar (Duplicate address detection) på frågan ”Vilken Neighbor Discovery-process kan utnyttjas av en angripare för att göra nätverket otillgängligt för nya värdar som skall ansluta till nätverket?” Med detta resultat kan slutsatsen dras att medvetenheten om denna risk är väldigt låg. Majoriteten av deltagarna har dock uttalat sin okunskap.

**Figur 8** Risk med fragmentering

**Figur 9** Risk med Duplicate adress detection
5.2.5 Medvetenhet om risk med standardroutern
30 % av respondenterna (se Figur 10) har angett det korrepta svarsalternativet (Förfalska Router Advertisements med parametern Router Lifetime satt till 0) på frågan ”Vilken av följande metoder kan användas för att göra standardroutern i nätverket onåbar?” Detta indikerar en låg medvetenhet samtidigt som samtliga deltagare medger att de inte har kunskap om risken.

**Figur 10** Risk med standardroutern

5.2.6 Medvetenhet om risk med Hop-by-hop options header
På frågan ”I vilken Extension Header kan en angripare infoga inkonsistenta alternativa värden eller ogiltiga alternativ och få en stor mängd ”Parameter Problem” ICMPv6 error-meddelanden att skickas till routrar och på så sätt göra dem otillgängliga?” har endast 10 % (se Figur 11) av enkätens deltagare angett ett korrekt svar (Hop-by-hop Options), vilket tyder på att medvetenhet om denna risk är väldigt låg. Samtliga respondenter har angett att de gissade när de fyllde i sitt svar.
5.2.7 Medvetenhet om risk med granncache

40 % (se Figur 12) av enkätens deltagare har angett rätt svarsalternativ (En angripare kan genom att skicka förfalskade Neighbor Advertisements skriva över mappningar mellan IP-adress och MAC-adress) på frågan ”På vilket sätt kan granncachen hos en värd modifieras av en angripare?” Detta ger en antydning om att det finns en viss medvetenhet hos deltagarna, men alla respondenten har angivit att de har gissat på frågan. Vidare eftersom det bara finns tre svarsalternativ så borde i medel drygt 33 % svara rätt även om de inte har någon aning om svaret, vilket endast är 7 procentenheter mindre än 40 %. På grund av detta är medvetenheten dock troligtvis ändå låg.

![Figur 11 Risk med Hop-by-hop options header](image-url)
5.2.8 Medvetenhet om risk med tunnlingsmekanismer

På frågan om "Varför är 6to4-arkitekturen sårbar för attacker?" har 50 % (se Figur 13) angett ett korrekt svar (Alla 6to4-routrar måste acceptera och dekapsulera IPv4-paket från vilken adress som helst). Detta tyder på en viss kunskap om denna säkerhetsrisk, men 80 % har angett att de har gissat så antagligen är medvetenhet ändå låg.
5.2.9 Medvetenhet om risk med autokonfiguration

40 % av respondenterna (se Figur 14) har angett ett korrekt svar (Prefix Information) på frågan om "Vilken parameter kan en angripare använda sig av när den skickar förfalskade Router Advertisements för att få nya värder att erhålla adresser som inte är giltiga för nätverket?" Detta ger en antydning om att det finns en viss medvetenhet hos respondenterna, men alla respondenter har angivit att de har gissat på frågan. Till följd av detta är medvetenhet troligtvis låg.

Figur 13 Risk med tunnlingsmekanismer

Figur 14 Risk med autokonfiguration
5.2.10 Medvetenhet om risk med felaktigt prefix i det lokala nätverket
På frågan om ”Vilket Neighbor Discovery Protocol-meddelande kan förfalskas för att få värder i det lokala nätverket att tro att ett prefix finns i det lokala nätverket fastän det inte gör det?” angav endast 20 % (se Figur 15) det korrektta svaret (Router Advertisement). Vidare angav alla deltagare att de gissade. Därmed tyder resultatet på denna fråga att svarsdeltagarna har en låg medvetenhet om denna risk.

![Figur 15 Risk med felaktigt prefix i det lokala nätverket](image)

5.2.11 Medvetenhet om risk med adresser för ett givet prefix
60 % av deltagarna (se Figur 16) i undersökningen har angett rätt svar (Skicka trafik till påhittade adresser med det aktuella nätverkets subnätsprefix) på frågan ”Hur kan routern som förekommer sist innan destinationens slutmål göras otillgänglig, då den är upptagen med att skicka Neighbor Solicitations?” Detta indikerar en acceptabel medvetenhet om denna säkerhetsrisk, men å andra sidan har 90 % av alla deltagare gissat. Av denna anledning är medvetenheten även på denna fråga förmodligen låg.
Figur 16 Risk med adresser för ett givet prefix

5.2.12 Medvetenhet om risk med ICMPv6

På frågan om "Vilken av följande egenskaper gör ICMPv6 sårbart för Denial of Service-attacker?" angav 60 % (se Figur 17) det korrekta svaret (Vissa typer av meddelanden måste tillåtas för att nätverket skall fungera korrekt). Här angav även 40 % av deltagarna att de var ganska säkra på sina svar, vilket tillsammans med 60 % korrekta svar antyder att det finns en viss medvetenhet om denna risk hos systemadministratörerna som deltog i enkäten. Vidare då det finns fyra svarsalternativ så bör i medel drygt 25 % svara rätt även om de inte har någon aning om det korreka svaret. 60 % är 35 procentenheter större än 25 %. Detta ger också en antydan om det finns en viss medvetenhet om denna risk.
Utifrån en analys av enkätens resultat kan slutsatsen dras att de som har besvarat enkäten har uppvisat en låg medvetenhet om de olika säkerhetsriskerna gällande tillgänglighet som förekommer vid en övergång till IPv6.


De som inte har erfarenhet av IPv6 får i medel 3,625 rätt medan de som har erfarenhet av IPv6 i medel får 3,5 rätt. Detta tyder på att erfarenhet av att administrera nätverk där IPv6 används inte påverkar medvetenheten om de identifierade riskerna.

**Figur 17** Risk med ICMPv6

**5.2.13 Sammanfattande analys**

Utifrån en analys av enkätens resultat kan slutsatsen dras att de som har besvarat enkäten har uppvisat en låg medvetenhet om de olika säkerhetsriskerna gällande tillgänglighet som förekommer vid en övergång till IPv6.
**Figur 18** Antal rätta svar i förhållande till angiven erfarenhet av IPv6

Vidare tyder resultaten på att systemadministratörerna inte tror att de har mer kunskap än vad de egentligen har. Detta på grund av att svarsalternativet ”Helt säker” aldrig har valts på någon fråga, ”Ganska säker” endast ett fåtal gånger och ”Svaret var en gissning” har valts i en klar majoritet av fallen. Dessutom har en respondent uppgivit i den övriga delen av enkäten att han eller hon bör läsa på mer om NDP. Figur 19 visar att antalet rätta svar ökar då gissningarna minskar.

**Figur 19** Antal rätta svar i förhållande till antalet gissningar

Slutligen illustrerar Figur 20 att antalet rätta svar är fler om utbildningsnivån är högre. Den person som har flest antal rätta svar har den högsta utbildningsnivån samtidigt som trendlinjen i Figur 20 visar att antalet rätt ökar med högre utbildningsnivå. Högre utbildning ger alltså en bättre förmåga att besvara frågorna korrekt i enkäten.
Figur 20 Antal rätta svar i förhållande till utbildning
6 Slutsats och diskussion

Detta kapitel presenterar inledningsvis de slutsatser som har dragits utifrån de resultat och analyser som presenterades i kapitel 5. Uppfyllandet av rapportens frågeställning och delmål diskuteras också. Därefter följer en diskussion och slutligen beskrivs möjligheter till framtida arbete.

6.1 Slutsats

Frågeställningen som arbetet hade var "Vilka säkerhetsrisker gällande tillgänglighet finns vid en övergång från IPv4 till IPv6 och vilken medvetenhet om dessa har systemadministratörer?" Denna frågeställning delades upp i tre delmål.

**Delmål 1: Identifiera och sammanställa de olika säkerhetsriskerna gällande tillgänglighet som finns vid en övergång till IPv6.**


**Delmål 2: Undersök systemadministratörers medvetenhet om de säkerhetsrisker gällande tillgänglighet som uppkommer vid en övergång till IPv6.**


**Delmål 3: Jämföra och sammanställa resultaten från de föregående delmålen och dra slutsatser utifrån dessa.**

Det tredje delmålet har uppfyllts då resultaten från de två första delmålen har jämförts och sammanställts och slutsatser har dragits utifrån dessa. slutsatser om medvetenheten i denna undersökning har fastställts och djupare analyser på medvetenheten efter de initiala resultaten har utförts.

Sammanfattningsvis tyder de erhållna delresultaten på att frågeställningen som helhet är besvarad då tolv olika säkerhetsrisker gällande tillgänglighet med IPv6 har identifierats samt att medvetenheten om dessa har undersöks hos systemadministratörer (dock ett begränsat svarsunderlag).
6.2 Diskussion


I detta arbete utnyttjades två olika metoder, vilka var litteraturstudie och enkätundersökning. Som tidigare nämnts i delkapitel 4.1 brukar enkätundersökningar ofta ge låga svarsfrekvenser. Detta problem uppstod i detta arbete då endast 10 av 90 erbjudna deltagare på högskolor runt om i landet valde att genomföra enkäten. Trots påminnelser blev alltså svarsfrekvensen endast cirka 11 %, vilket gör att resultaten inte är tillförlitliga. Därmed kan inte alltför stora slutsatser dras med säkerhet. Med tanke på att enkätens genomförande och utformning har beskrivits i detalj i denna rapport bör det vara enkelt att återupprepa enkätundersökningen eftersom den finns i Bilaga B.

Enkäten skulle istället för att likna en quiz kunna ha utformats med frågor som ”Känner du till denna risk?” Det utfördes inte då detta avgör respondentens egen uppskattnings av sin medvetenhet om de olika riskerna istället för respondentens faktiska medvetenhet, vilket var vad frågeställningen syftade till att undersöka.

Vidare kan någon eller några av frågorna som har framtagits vara felaktigt formulerad. Det kan vara så att någon fråga har mer än ett korrekt alternativ. Detta på grund av att nya sårbarheter kan ha upptäckts sedan de vetenskapliga artiklarna som enkäten baserades på skrevs och mer eller nyupptäckt information kan ha presenterats i andra källor som till exempel inte är vetenskapliga. Det anses omöjligt att genom att avancerade all information om risker med IPv6 som finns under detta arbetes tidsspann. För att minimera risken att frågorna är felaktigt formulerade har dock en granskning av de berörta protokollen utförts.

En kompletterande eller alternativ metod skulle kunna ha varit intervju som tas upp i kapitel 4.1, men intervjunet domen valdes bort på grund av tidsbrist. I efterhand skulle denna metod kunna ha varit ett bra komplement till enkäten. Genom att använda sig utav både en enkät och en intervju kunde enkäten kanske deltaganteralet kunde ha ökats, då människor ofta kan vara villigare att delta vid en mer personlig kontakt, samt att trovärdigheten för studiens resultat skulle kunna ha ökat, givet möjligheten till metodtriangulering (att använda sig av flera olika metoder för att besvara en frågeställning (Repstad, 1999)).

Det är också möjligt någon säkerhetsrisk inte längre är aktuell på grund av att en lösning nyligen har implementerats. Uppdateringar till operativsystem och dylikt görs tillgängliga med jämna mellanrum. Även de säkerhetsrisker med IPv6 som har presenterats i denna rapport så finns liknande eller motsvarande risker i IPv4 när det gäller riskerna om fragmentering och granncache. De övriga riskerna som har presenterats har egentligen ingen motsvarighet i IPv4. Reconnaissance (spaning) i form av till exempel portskanning (undersökning av vilka tjänster som det är möjligt att ansluta till hos en värd) är en vanlig säkerhetsrisk i IPv4, men i och med IPv6 och dess enorma antal adresser kommer denna risk med stor sannolikhet att bli inaktuell, då det kommer ta väldigt lång tid att bara hitta en enstaka aktiv värd bland alla möjliga adresser.


6.3 Framtida arbete

Nedan ges exempel på fortsatta studier som kan vara intressanta att arbeta med i framtiden för att komplettera eller utöka resultaten som har presenterats i denna rapport:

- En undersökning som har ett större deltagarantal från olika typer av organisationer som undersöker medvetenheten om säkerhetsrisker gällande tillgänglighet som förekommer vid en övergång från IPv4 till IPv6.

- Ett arbete som undersöker vilka säkerhetsrisker gällande andra informationssäkerhetsaspekter (integritet, konfidentialitet et cetera) som finns vid en övergång från IPv4 till IPv6 och vilken medvetenhet systemadministratörer har om dessa.

- En undersökning som undersöker systemadministratörers medvetenhet om säkerhetsrisker vid övergången från IPv4 till IPv6 och jämför detta med hur utbrett IPv6 är. Har systemadministratörer som arbetar dagligen med nätverk där IPv6 används en tillräckligt bra medvetenhet?

- Undersöka hur systemadministratörer kan utbildas på bästa sätt för att deras medvetenhet om säkerhetsriskerna skall öka.

- Undersöka hur de berörda protokollen kan förändras för att motverka riskerna.
Referenser


Stiftelsen för Internetinfrastruktur (2012) *Ny undersökning visar hur införandet av IPv6 i Sverige går*. Tillgänglig på Internet: https://www.iis.se/blogg/inforandet-av-ipv6-i-sverige [Hämtad 12.05.30].


Bilaga A - Inbjudan till enkät

Hej!


Ett stort tack på förhand för din medverkan!

Enkäten hittas på följande länk:
https://docs.google.com/spreadsheet/viewform?formkey=dHY1aXgyREliU3AtekE2TFlya000REE6MQ

Marcus Karlsson, Högskolan i Skövde
Bilaga B - Enkäten

Del 1 Inledande frågor

1. Vilket år är du född? (åååå)
   ____

2. Vilken utbildningsnivå har du?
   a) Förgymnasial
   b) Gymnasial högst 2 år
   c) Gymnasial mer än 2 år
   d) Eftergymnasial mindre än 3 år
   e) Eftergymnasial minst 3 år

3. Vilket år började du arbeta som systemadministratör? (åååå)
   ____

4. Har du administrerat nätverk där IPv6 används?
   a) Ja
   b) Nej

Del 2 Säkerhetsrisker

1. Vilken IPv6 Extension Header kan av en angripare utnyttjas för att undvika accesskontroller som filtrerar på destinationsadress?
   a) Hop-By-Hop Options
   b) Routing
   c) Fragment
   d) Encapsulating Security Payload
   e) Authentication Header
   f) Destination Options

2. Hur säker är du på att ditt svar på föregående fråga (fråga 1) är korrekt?
   a) Helt säker
   b) Ganska säker
3. Vilken IPv6 Extension Header kan av en angripare utnyttjas för att utföra Denial of Service-attacker genom att förfalska paket och omdirigera dem genom värdar med publika IP-adresser?
   a) Hop-By-Hop Options
   b) Routing
   c) Fragment
   d) Encapsulating Security Payload
   e) Authentication Header
   f) Destination Options

4. Hur säker är du på att ditt svar på föregående fråga (fråga 3) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

5. Med vilken av följande metoder kan en angripare undvika accesskontroller?
   a) Skicka fragmenterade paket där det första fragmentet saknar portnummer (paketet sammansätts inte av mottagande enhet)
   b) Skicka fragmenterade paket där det sista fragmentet saknar portnummer (paketet sammansätts inte av mottagande enhet)
   c) Skicka fragmenterade paket där alla utom det första fragmentet saknar portnummer (paketet sammansätts inte av mottagande enhet)

6. Hur säker är du på att ditt svar på föregående fråga (fråga 5) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

7. Vilken av följande egenskaper gör ICMPv6 sårbart för Denial of Service-attacker?
   a) Alla olika typer av meddelanden måste tillåtas för att nätverket skall fungera korrekt
   b) Vissa typer av meddelanden måste tillåtas för att nätverket skall fungera korrekt
   c) ICMPv6-meddelanden kan skickas till anycast-adresser
8. Hur säker är du på att ditt svar på föregående fråga (fråga 7) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

9. Vilken Neighbor Discovery-process kan utnyttjas av en angripare för att göra nätverket otillgängligt för nya värder som skall ansluta till nätverket?
   a) Duplicate address detection
   b) Address resolution
   c) Router discovery
   d) Redirect function

10. Hur säker är du på att ditt svar på föregående fråga (fråga 9) är korrekt?
    a) Helt säker
    b) Ganska säker
    c) Svaret var en gissning

11. Vilken av följande metoder kan användas för att göra standardroutern i nätverket onåbar?
    a) Förfalska Router Advertisements med parametern Router Lifetime satt till 0
    b) Förfalska Router Advertisements med parametern Router Lifetime satt till 1
    c) Förfalska Router Solicitations
    d) Förfalska Neighbor Solicitations

12. Hur säker är du på att ditt svar på föregående fråga (fråga 11) är korrekt?
    a) Helt säker
    b) Ganska säker
    c) Svaret var en gissning

13. I vilken Extension Header kan en angripare infoga inkonsistenta alternativa värden eller ogiltiga alternativ och få en stor mängd ”Parameter Problem” ICMPv6 errormeddelanden att skickas till routrar och på så sätt göra dem otillgängliga?
    a) Hop-By-Hop Options
    b) Routing
c) Fragment
d) Encapsulating Security Payload
e) Authentication Header

14. Hur säker är du på ditt svar på föregående fråga (fråga 13) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

15. På vilket sätt kan granncachen hos en värd modifieras av en angripare?
   a) En angripare kan genom att skicka endast en förfalskad Neighbor Advertisement tömma hela värdens granncache
   b) En angripare kan genom att skicka förfalskade Neighbor Advertisements skriva över mappningar mellan IP-adress och MAC-adress
   c) En angripare kan genom att skicka endast en förfalskad Neighbor Advertisement skriva över hela värdens granncache med felaktiga värden

16. Hur säker är du på att ditt svar på föregående fråga (fråga 15) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

17. Varför är 6to4-arkitekturen sårbar för attacker?
   a) Alla 6to4-routrar måste acceptera och dekapsulera IPv4-paket från vilken adress som helst
   b) Det är inte möjligt att använda accesslistor för att filtrera trafik
   c) Det är omöjligt att avgöra om den inbäddade IPv4-adressen är en giltig global unicast-adress

18. Hur säker är du på att ditt svar på föregående fråga (fråga 17) är korrekt?
   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning
19. Vilken parameter kan en angripare använda sig av när den skickar förfalskade Router Advertisements för att få nya värdar att erhålla adresser som inte är giltiga för nätverket?

   a) Prefix Information
   b) Router Lifetime
   c) Reachable Time
   d) Source Link-Layer Address

20. Hur säker är du på att ditt svar på föregående fråga (fråga 19) är korrekt?

   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

21. Vilket Neighbor Discovery Protocol-meddelande kan förfalskas för att få värdar i det lokala nätverket att tro att ett prefix finns i det lokala nätverket fastän det inte gör det?

   a) Router Solicitation
   b) Router Advertisement
   c) Neighbor Advertisement
   d) Neighbor Solicitation

22. Hur säker är du på att ditt svar på föregående fråga (fråga 21) är korrekt?

   a) Helt säker
   b) Ganska säker
   c) Svaret var en gissning

23. Hur kan routern som förekommer sist innan destinationens slutmål göras otillgänglig, då den är upptagen med att skicka Neighbor Solicitations?

   a) Skicka förfalskade Neighbor Solicitations
   b) Skicka förfalskade Router Solicitations
   c) Skicka förfalskade Router Advertisements
   d) Skicka trafik till påhittade adresser med det aktuella nätverkets subnätsprefix

24. Hur säker är du på att ditt svar på föregående fråga (fråga 23) är korrekt?
a) Helt säker
b) Ganska säker
c) Svaret var en gissning

Del 3 Övrigt

Har du något övrigt att tillägga?

________________________________________

________________________________________
IPv6 säkerhetsrisker

Denna enkät består av tre delar som jag är väldigt tacksam om du tar dig tid att besvara:

Första delen - Generella frågor om dig
Andra delen - Frågor som syftar till att testa kunskaper om säkerhetsrisker
Sista delen - Del där övriga kommentarer kan infogas

Enkäten är anonym och det är viktigt att du inte tar hjälp av andra efter att du själv när frågorna besvaras.

Från Google Dokument

Anmärkningar ändrar sig. Användarvillkor. Ytterligare villkor

IPv6 säkerhetsrisker

*Obligatorisk

Del 1 Inledande frågor

<table>
<thead>
<tr>
<th>Fråga 1 *</th>
<th>Vilket år är du född? (År)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Fråga 2 *</th>
<th>Vilken utbildningsnivå har du?</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Förgymnasial</td>
<td></td>
</tr>
<tr>
<td>☐ Gymnasial högst 2 år</td>
<td></td>
</tr>
<tr>
<td>☐ Gymnasial mer än 2 år</td>
<td></td>
</tr>
<tr>
<td>☐ Eftergymnasial mindre än 3 år</td>
<td></td>
</tr>
<tr>
<td>☐ Eftergymnasial minst 3 år</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fråga 3 *</th>
<th>Vilket år började du arbeta som systemadministrator? (År)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Fråga 4 *</th>
<th>Har du administrerat nätverk där IPv6 används?</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Ja</td>
<td></td>
</tr>
<tr>
<td>☐ Nej</td>
<td></td>
</tr>
</tbody>
</table>

« Bakåt »  « Fortsett »

Från Google Dokument

Anmärkningar ändrar sig. Användarvillkor. Ytterligare villkor
**IPv6 säkerhetsrisker**

*Obligatorisk*

**Del 2 Säkerhetsrisker**

<table>
<thead>
<tr>
<th>Fråga 1</th>
<th>Villken IPv6 Extension Header kan av en angripare utnyttjas för att undvika accesskontroller som filtrerar på destinationsadress?</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Hop-By-Hop Options</td>
<td></td>
</tr>
<tr>
<td>☐ Routing</td>
<td></td>
</tr>
<tr>
<td>☐ Fragment</td>
<td></td>
</tr>
<tr>
<td>☐ Encapsulating Security Payload</td>
<td></td>
</tr>
<tr>
<td>☐ Authentication Header</td>
<td></td>
</tr>
<tr>
<td>☐ Destination Options</td>
<td></td>
</tr>
</tbody>
</table>

**Fråga 2**

Hur säker är du på att ditt svar på föregående fråga (fråga 1) är korrekt?

- ☐ Helt säker
- ☐ Ganska säker
- ☐ Svaret var en gissning

**Fråga 3**

Vilken IPv6 Extension Header kan av en angripare utnyttjas för att utföra Denial of Service-attackar genom att förfalska paket och omdirigera dem genom värden med publika IP-adresser?

- ☐ Hop-By-Hop Options
- ☐ Routing
- ☐ Fragment
- ☐ Encapsulating Security Payload
- ☐ Authentication Header
- ☐ Destination Options

**Fråga 4**

Hur säker är du på att ditt svar på föregående fråga (fråga 3) är korrekt?

- ☐ Helt säker
- ☐ Ganska säker
- ☐ Svaret var en gissning
IPv6 säkerhetsrisker

Del 3 Övrigt

Fråga 1

Har du något övrigt att tillägga?

...