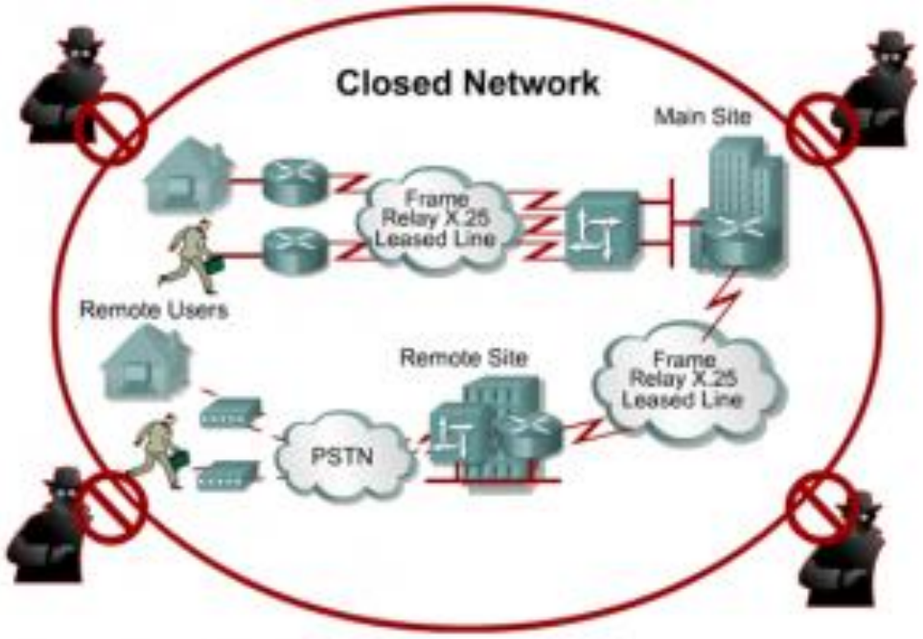
Nätverkssäkerhet

Nätverkssäkerhets grunder

Vad innebär nätverkssäkerhet?

- Tillämpning av protokoll, teknik, verktyg och säkerhetsmekanismer implementerade i mjukvara och hårdvara.
- Nätverkssäkerhets syfte att skydda nätverket och dess fysiska komponenter genom att placera dessa på speciella platser där obehöriga åtkomst kan förhindras.
- Det handlar inte om att isolera ett nätverk.
- Det handlar att hålla bort obehörig åtkomst, att skydda nätverket med robusta system.
- Det handlar om att förebygga eventuella attacker och minimera realtidsattackers effekt.
- Tre viktiga principer:
  - Prevention
  - Detection
  - Reaction



Organisationers verksamhet

- Nätverkssäkerhet har ett direkt samband med organisationers verksamhet.
- Attacker till en organisationsverksamhet kan leda till förlorade intäkter för företag, stöld av intellektuell egendom, juridiska konflikter, och kan även hota den allmänna säkerheten.
- Attacker till länder är idag inte längre små utan i stor skala.
- Angriparna använder ofta DoS-attacker som styr stora mängder datatrafik mot landets myndigheters webbplatser som till slut kraschar av överbelastning.
- SVT nyheterna publicerade den 5 juli 2021 följande rubrik:
- ***Coop-butikerna har tvingats hålla stängt hela helgen för att de inte kan ta betalt. Nu kräver hackergruppen Revil 598 miljoner kronor för att släppa IT-systemen som Coop och andra företag över hela världen är beroende av.***
- USA:s president Joe Biden varnar för att omfattande hackerattacker mot USA skulle kunna leda till fullskaligt krig, där Kina och Ryssland ses som växande hot.

Nätverksrisker

- På många håll i världen pågår nu tester med både mindre lastbilar på korta rutter och riktigt tunga fordon som redan i dag kan köra hundratals mil utan förare.
- I Norden har bolaget Einride fått mycket uppmärksamhet för sin banbrytande Pod – en förarlös och fjärrövervakad mindre lastbil som dessutom är eldriven.
- Podden testades för första gången på DB Schenker i Jönköping 2019.
- Sedan dess har stora företag som Axfood, Coca-Cola och Lidl börjat använda den för kortare transporter mellan lager och terminaler.
- 802.11p standard befinner sig i intensiv utveckling.
- Men….
- Varje fordon är i praktiken en mobil dator
- och datorer hackas dagligen!

Professionella säkerhetsspecialister

- För att garantera säkerhet i ett nätverk krävs professionella yrkeskunniga säkerhetsspecialister som ska ständigt vara medvetna om nya och framväxande hot och attacker till nätverk.
- Nätverkssäkerhetsspecialister har fördjupade kunskaper inom nätverk, programmering, databas, IT-management och inte minst säkerhet.
- Säkerhetsspecialister har som utgångspunkt i *att skydda de mest sårbara enheter, nätverksanvändare och deras hjälpmedel som kör applikationer*.
- Vid landnivå är ingen nyhet att flera länder, inklusive Sverige, rekryterar hackare så att speciella styrkor organiseras med syfte att skydda deras länder.

Risker på Internet

Dataintrång

- Dataintrång innebär att man utan tillstånd väljer att ge sig själv tillgång till information som lagras digitalt.
- Med åtkomst till digital information kan man ändra, ta bort eller lägga till ytterligare information utan tillstånd.
- Dataintrång är så klart brottsligt.
- Polisen yttrar sig på sin hemsida över IT-relaterade brott:
- *Idag är de flesta brott IT-relaterade på något sätt. Per definition är IT-brott dataintrång och datorbedrägeri, men det finns flera andra brott som är direkt kopplade till IT och sociala medier.*

Nätverksrisker

- I slutet av 1990-talet och början av 2000-talet blev det en markant ökning av antalet datavirus, men fortfarande handlade det om att få berömmelse.
- Hur kom det sig att Internet är full av kriminella rörelser?
- Dagens attackmetoder har blivit destruktiva och kriminella därav mer komplexa/avancerade.
- Attackmetoder förändras ständigt och nya dyker upp hela tiden.
- Det är svårt att kartlägga vem eller vilka som kommer att attackera ett nätverk.
  - Terrorister
  - Kriminella
  - Missnöjda anställda
  - Konkurrenter
  - Någon som har tillgång till en datorutrustning
  - Statliga säkerhetsspecialister
  - Hackerarme

Säkerhetshål - Vulnerability

- “Fel i systemet” uppfattas som potentiella risker.
- Säkerhetshål i hårdvarutillverkning, ta som exempel Realtek trådlöst nätverkskort.
- Realtek levererar WiFi kretsar till produkttillverkare som tillverkar alltifrån routrar till smarta hem-prylar.
- Säkerhetsmässiga sårbarhet har upptäckts i programkod från den taiwanesiska underleverantören Realtek.
- Det drabbar ett stort antal trådlöst uppkopplade elektronikprylar från minst 65 olika tillverkare.
- Produkttillverkarna använder Realteks mjukvara som grund för mjukvaran som deras egna produkter kör.

Säkerhetsorganisationer

SANS

- SANS grundades 1989 som ett forskningssamarbete och utbildningsorganisation.
- SANS är den mest betrodda och den i särklass största källan för säkerhetsutbildning och säkerhetscertifiering i världen.
- Organisationen utvecklar, underhåller och gör tillgängligt för allmänheten den största samlingen av forskningsdokument om olika aspekter inom informationssäkerheten.
- SANS driver flera Internet Portaler relaterade till informationssäkerhet exempelvis Internets alarmsystem känd som *Internet Storm Center*, Cyber Defense, Penetration Testing.
- SANS tillhandahåller online och gratis kurser: Cyber Aces Online.
- SANS utvecklar säkerhets kurser för certifikatet *GIAG*, Global Information Assurance Certification.
- Analys, intrångsdetektering, incidenthantering, brandväggar och skalskydd mot hacking.

CERT – Computer Emergency Response Team

- CERT var grundad av Defense Advanced Research Projects Agency (DARPA) som en reaktion till Morris masken (1988).
- CERT hantering av säkerhetsproblem inom Cybersäkerhet och fokuserar mest på DoS incidenter.
- I Sverige CERT-SE har för uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.
- Incidenthanteringen omfattar fem steg:
  - att förebygga, identifiera, begränsa, återställa och samla erfarenheter.
- Till uppgifterna hör bland annat att:
  - *Agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.*
  - *Samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.*
  - *Vara Sveriges kontaktpunkt samt utveckla samarbetet och informationsutbytet med andra länder.*

Andra säkerhetsrelaterade organisationer

- Det finns en uppsjö av organisationer med fokus på information-, nätverks- och cybersäkerhet:
- *The Mitre Corporation* upprätthåller en förteckning över Common Vulnerabilities and Exposures (CVE) (lexikon) som används av framträdande säkerhetsorganisationer.
- *Forum for Incedent Response and Security Teams* (FIRST) är en säkerhetsorganisation som samlar en mängd olika datasäkerhetsincidenter från regeringen, kommersiella och utbildningsorganisationer för att främja samarbete och samordning i informationsutbytet, incident förebyggande och snabb reaktion.
- *Center for Internet Security* (CIS) är en icke-vinstdrivande företag som utvecklar nationella säkerhetskonfigurationer genom en global konsensus för att minska risken för affärs- och e-handel.

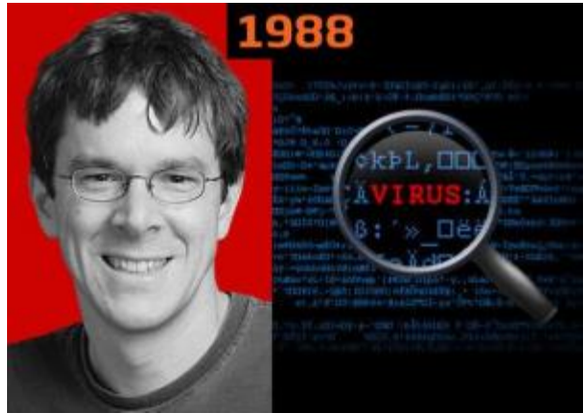
Malware

Malware – skadlig programvara

- Termen ”*malware*” är en kombination av orden ”*malicious*” och ”*software*”
- Kriminella gör sitt yttersta för att ta kontroll över din dator och utnyttja den på olika sätt.
- exempelvis spionera på din aktivitet, stjäla användaruppgifter, hota att avslöja personliga uppgifter, kräva pengar eller använda ditt system för att attackera andra.
- Packed malware är en avancerat skadligt program som undviker detektorer, komprimerar och krypterar filer.
  - **Computer viruses**
  - **Trojaner**
  - **Maskar**
  - **Spyware**
  - **Ransomware**
  - **Adware**
  - **Scareware**
  - **Packed**
  - **Maldoc**
  - **Logic bomb**

Begrepp

- Definitioner jag använder hämtar jag från en Internet-guide från Daniel Goldberg och Linus Larsson.
- *Datorvirus/datavirus*
- En skadlig kod som är kopplad till legitima program eller körbara filer.
- De flesta datavirus kräver aktivering genom en association till annat program.
- Ett datavirus kan lägga sig vilande under en längre period och sedan kan det aktiveras vid en viss tidpunkt eller datum (logisk bomb).
- *Worms eller maskar*
- Fristående program som inte behöver infektera filer eller program för att existera.
- En mask exekverar själv godtycklig kod och installerar kopior av sig själv i minnet av den infekterade datorn.
- Därefter skannar masken nätverket och söker öppna utgångar så att den kan sprida sig vidare.

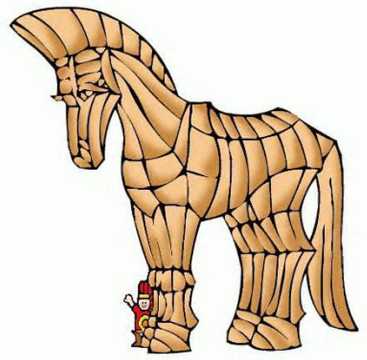


Begrepp

- *Trojan Horse*
- Skadlig programvara som ofta låtsas vara legitim.
- Användarna blir ofta lurade att läsa in och köra trojaner på datorerna med någon typ av social manipulation.
- När trojanerna är aktiverade kan cyberbrottslingar spionera på dig, stjäla känsliga uppgifter och skapa bakdörrar in i systemet.
- Trojaner kan:
  - Ta bort data
  - Blockera data
  - Ändra data
  - Kopiera data
  - Störa funktionen för datorer eller datornätverk

Begrepp

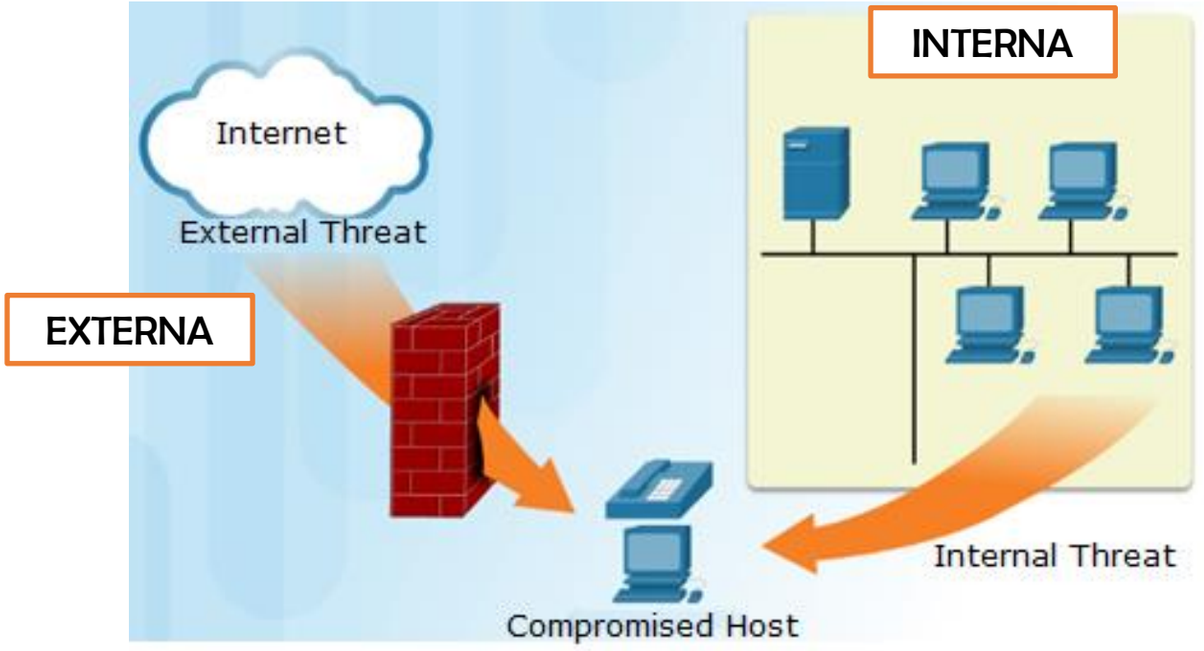
- Trojanska hästar efter skador de orsakar eller det sätt på vilket de bryter mot ett system:
  - *Remote-access Trojan* – möjliggör obehörig fjärråtkomst
  - *Data sändare Trojan* – ger angriparen känsliga uppgifter såsom lösenord
  - *Destruktiva Trojan* – korrumperar eller raderar filer
  - *Proxy Trojan* – användarens dator fungerar som en proxyserver
  - *FTP Trojan* - Öppnar port 21
  - *Säkerhetsprogram Trojan* – stoppar antivirusprogram eller brandväggar
  - *Denial of Service Trojan* – bromsar eller stoppar nätverksaktivitet
  - *Nätverksspelstrojaner* - stjäl användares kontoinformation.
  - *Utpressningstrojaner* - låser upp dina data enbart efter att du har betalat den lösensumma de kräver.
  - *Spiontrojaner* - kan spionera på hur du använder din dator
  - *E-postinsamlande trojaner* - kan hämta e-postadresser från din dator.
- *Zeus Trojan* - En otäck liten trojan som har använts av botnet-operatörer runt om i världen.
- Med Zeus kan man stjäla bankuppgifter och andra personuppgifter, och trolig andra kriminella handlingar.



Attackmetoder

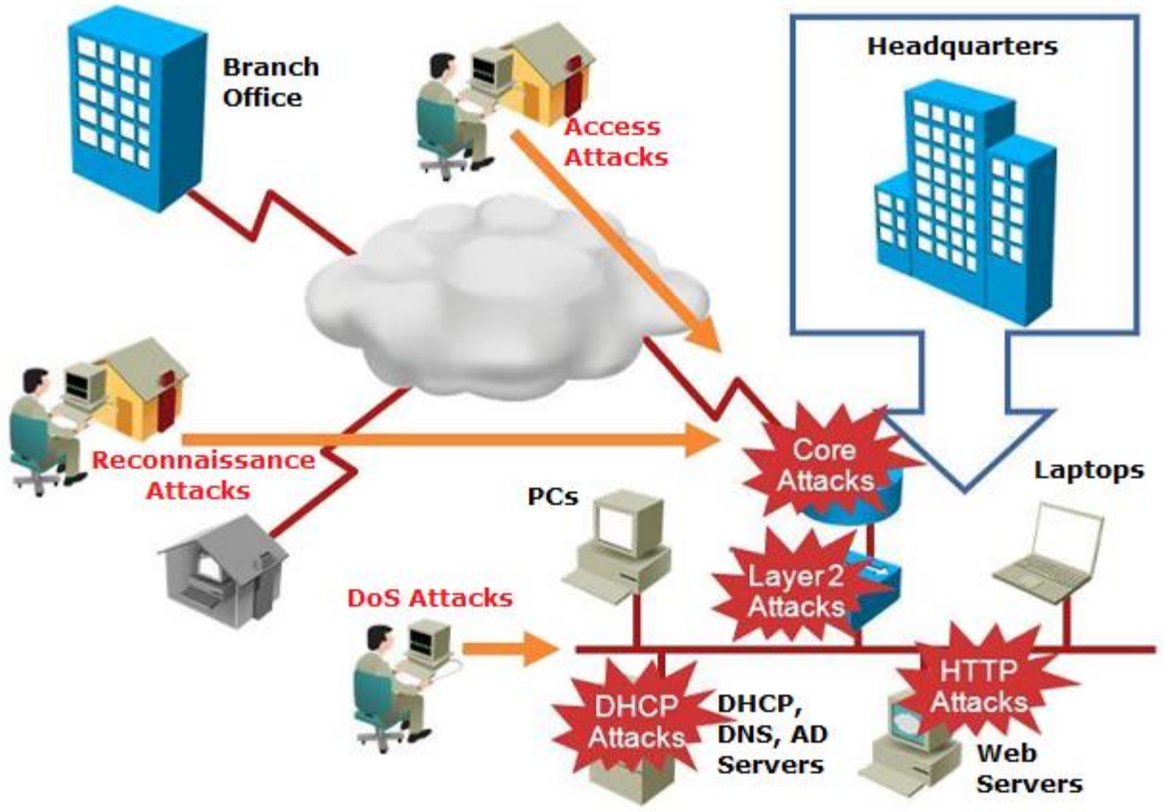
Attackmetoder

- Eller attackvektorer är olika sätt på vilka hacker kan få åtkomst till en server, resurs eller hela nätverk.
- Dessa vektorer kan grupperas i interna och externa.
- Till exempel en missnöjd anställ kan kopiera konfidentiella data och sälja den till konkurrenter.
- Samtidigt kan kompromissa interna servrar och nätverkets säkerhet.
- Allt dataintrång från Internet utnyttjar fel i nätverks säkerhetsinställningar.
- Det finns en uppsjö av attackmetoder av olika slag.



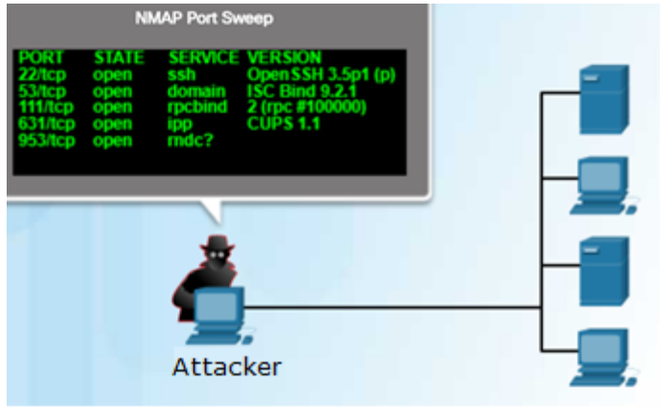
Attackmetoder

- För att mildra eller förhindra nätverksattacker är det nödvändigt att kategorisera först de olika typerna av attack.
- Här nedan anges ett exempel på kategorisering av attackmetoder:
  - spaningsattacker
  - åtkomstattacker
  - DoS attacker.
- Då blir det möjligt att analysera de och utveckla specifika säkerhetsmetoder.
- Flera begrepp, ibland på svenska och oftast på engelska.
- En webb sajt som tillhandahåller enkla men illustrerande definitioner är Computer Hope.



Spaningsattacker

- *Spaning* – att hitta information om ett visst nätverk/system.
- Detta är vanligtvis det första steget som tas för att upptäcka vad som finns på ett visst nätverk och för att identifiera eventuella sårbarheter.
- Dessa attacker använder ofta paketsniffare och port-skannrar.
- Följande verktyg kan användas för spaningsattacker:
  - *Packet sniffer* – använder nätverkskortet i promiscuous mode för att fånga alla nätverkspaket i ett nätverk. Det finns flera frikostnads applikationer som kan skanna datatrafiken exempelvis Wireshark.
  - *Ping sweep* (fping och andra liknande verktyg)
  - *Port scans* –man vill samla information om portar som lyssnar på specifika datatrafik.
  - *Internet information queries* – diverse web-baserade tjänster som tillhandahåller information om företag/organisationer och deras domäner associerade till IP-adresser.



Åtkomstattacker

- De utnyttjar kända sårbarheter i autentiseringstjänster, FTP-tjänster, webbtjänster, mm.
- En åtkomstattack kan utföras på många olika sätt.
  - *Lösenordsattacker* som genomförs med olika metoder inklusive brute-force. Brute-force baseras på inbyggda ordlistor för att identifiera användarkonto och lösenord. Lösenordsattacker kan genomföras med hjälp av trojaner, IP spoofing och Paketsniffare.
  - *Social ingenjörsteknik* – Det utnyttjar vår svagaste sårbarhet i ett säkert system, nämligen användaren.
  - *Nätfiske eller Phishing* – Det presenterar en länk som ser ut som en giltig pålitlig resurs till en användare.
  - *Pharming* – Orden *odling* och *nätfiske* motsvarar Pharming, en nätfiskebluff som kan drabba flera användare samtidigt. Pharming utnyttjar grunderna till hur man surfar på Internet.
    Hackaren har två alternativ för att utnyttja processen:
  - installera ett virus eller en trojan på användarens dator så att datatrafiken kan dirigeras om från det avsedda målet till en falsk webbplats.
  - förgifta en DNS-server och därigenom förmår flera användare att oavsiktligt besöka den falska webbplatsen.
  - De falska webbplatserna kan användas för att installera virus eller trojaner på användarens dator.

Social Engineering – Social manipulation

- Social Engineering, eller social ingenjörskonst på svenska, handlar om att manipulera människor så att de lämnar ifrån sig konfidentiell information.
- De som ägnar sig åt Social Engineering utger sig ofta för att vara en person med hög befogenhet som befinner sig i en tidspressad situation.
- Genom att låtsas att de behöver hjälp lurar de anställda så att de vinner tillträde till system eller information som de inte ska kunna komma åt.

Phishing - nätfiske

- Nätfiske är en attackmetod som går ut på att via mail, SMS, eller chatt lura mottagaren att öppna ett dokument, besöka en webbplats eller ladda ner en fil.
- Målet är att infektera enheten med skadlig kod och/eller komma över höga behörigheter.
- Några vanliga exempel på phishing är att:
  - En angripare utger sig för att vara en säkerhetsspecialist från en viss bank och ber mottagaren bekräfta kontouppgifter, annars spärras kortet.
  - En angripare utger sig för att vara från Skatteverket och uppmanar mottagaren att klicka på en länk för att få direkt tillgång till skatteåterbäringen.
  - En angripare utger sig för att jobba åt ett spelbolag och han vill berätta att mottagaren har vunnit en stor lotterivinst, men att det krävs vissa åtgärder för att lotterivinsten kunna betalas ut.

Åtkomstattacker

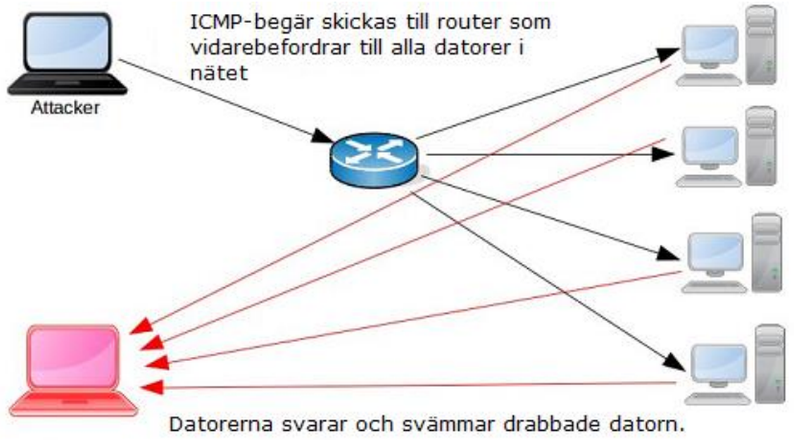
- En åtkomstattack kan utföras på många olika sätt.
  - *Kod-exekvering* – När angripare lyckas komma åt en nätverksenhet vill man oftast ha tillräckligt med behörighet så att kod i olika kommando kan exekveras.
  - *Man-in-the-middle* – Precis som det låter så är det en man ”i mitten” som utgör hotet: någon som tagit sig in mellan två parter som genomför en inloggning, utbyter information, avslutar en transaktion eller kanske byter lösenord.
  - *Port redirection –* På Host A, den svaga säkerhetslänken, kan installeras en applikation som omdirigerar datatrafik genom att manipulera port-numren.
  - *Trust exploitation* – som exempel kan beskrivas en situation där angriparen vill komma åt en målstation/server och därefter till en databas som innehåller information.
  - Servern skyddas av en brandvägg men inte datorer i samma nätverk som server finns i.
  - Angriparen inriktar sig till dator A och därefter till servern.

DoS attacker

- Överbelastningsattacker från en eller flera datorer.
- Orimliga antal förfrågningar tvingar systemet att arbeta kontinuerligt tills den kollapsar.
- Det attackerade system blir otillgängligt för legitim åtkomst och användning.
- DDoS-attack (Distributed Denial of Service attack)
- Ett stort antal datorer deltar i attacker till ett nätverk, en webbplats, mm.
- Paypal, Amazon, Visa, svenska banker, Arbetsförmedlingen, Polis, Telia och CNN är några exempel på företag och myndigheter som drabbats av en överbelastningsattack.
- 1: Kapa många uppkopplade datorer och skapa ett botnät.
- 2: Installera program i viloläge tills aktivering.
- 3: Initiera attacken
- 4: Generera ett stort antal anrop tills systemet slutar fungera.

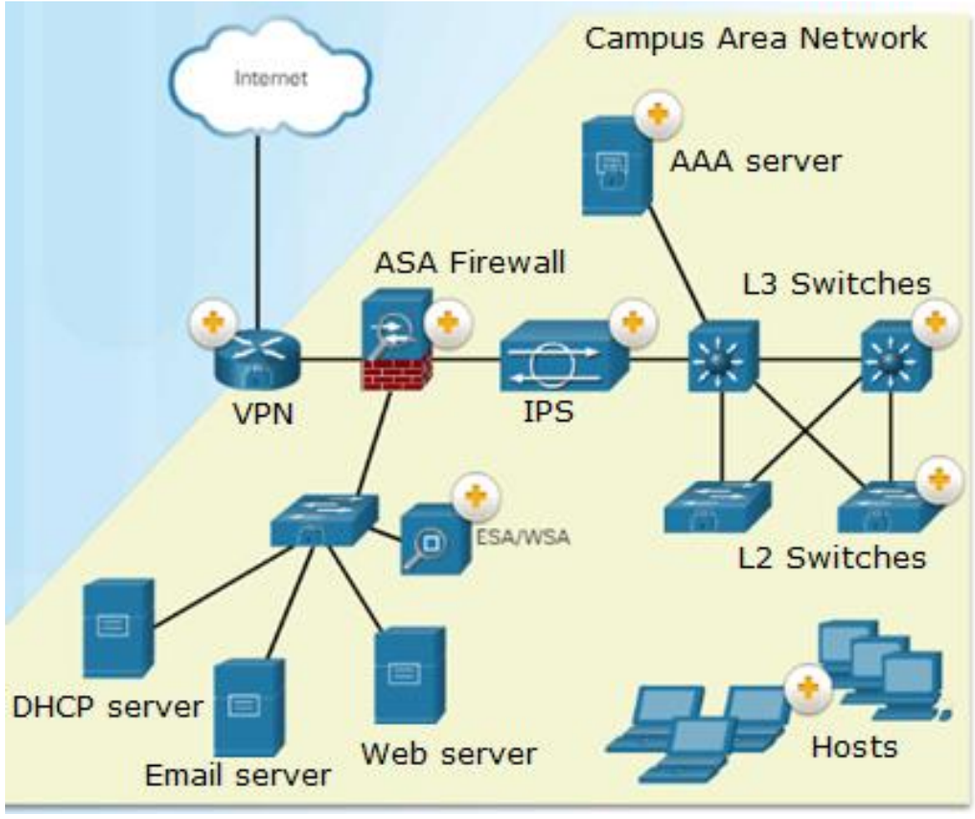
Botnet

- Det finns flera olika typer av DDoS attacker:
  - *Ping of Death* – att skicka stora paket via ping (ping -l 65600 hostIP)
  - Max storlek på ett paket är 65 535 bytes.
  - Istället kan skickas fraktioner av paket som innehåller ICMP begär
  - *Smurf Attack* – angriparen skickar ICMP förfrågningar via en broadcastadress till en router (amplifikations maskin) som vidarebefordrar till alla enheter anslutna till ett nätverk.
  - *TCP SYN Flood* – eller protokollutnyttjande attacker där klientdatorer begär kommunikation med en server och får en ACK paket tillbaka, men aldrig tackar ja paketet.



Campus nätverk

- Huvudfokus för denna kurs är att säkra ett Campus Area Networks (CAN).
- Ett campus nätverk består av sammankopplade LAN:s inom ett begränsat geografiskt område.
- Till exempel universitetsområden och företagsbyggnader.
- Nätverkspersonal måste implementera olika nätverkssäkerhetstekniker för att skydda organisationernas tillgångar utifrån och inuti hot.
- Anslutningar till otillförlitliga nätverk måste kontrolleras ingående av flera lager av försvar innan de når företagets resurser.
- Nätverksadministratörerna övervakar, tillåter och begränsar åtkomsten till ett campus nätverk.
- Externa anslutningar kräver VPN och brandväggar placeras vanligtvis mellan CAN och Internet för att skydda nätverket från obehörig åtkomst.
- IPS och IDS detektorer skyddar nätverket bakom brandväggen.



Nätverkssäkerhet