Nätverkssäkerhet

Nätverkssäkerhet eller Informationssäkerhet?

Vad vill vi skydda egentligen?

Dator- eller datavirus?

Vad innebär nätverkssäkerhet?

- Tillämpning av protokoll, teknik, verktyg och säkerhetsmekanismer.
- Förebygga eventuella attacker och minimera realtidsattackers effekt.
- Det handlar inte om att isolera ett nätverk.
- Det handlar att hålla bort obehörig åtkomst, att skydda nätverket med robusta system.
- Det gäller att hålla sig uppdaterad.
- Tre viktiga principer
- Prevention
- Detection
- Reaction

Att förstå grunder om Cybersäkerhet

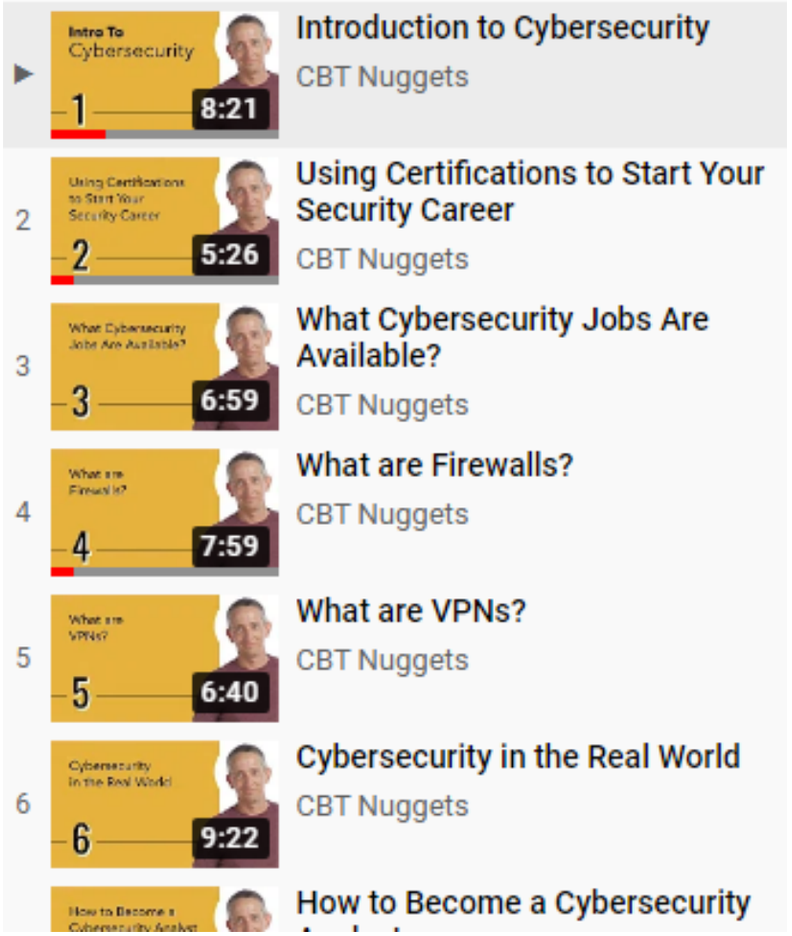
1. Vilka utövar egentligen ”hacking”
2. Vad är de efter?
3. Vilka faser att tänka på gällande cybersäkerhet?
4. Vad kan du göra i förebyggande fasen?
5. Vad är och gör FireEye?
6. https://www.youtube.com/watch?v=O5R4XHw0PQ0

Cisco Security

1. Vad för koncept har Cisco gällande säkerhet?
2. Vilka fyra säkerhetsprodukter ingår i SecureX plattform?
3. Hur säkrar Cisco ett nätverk?
4. Vilka Cisco produkter säkrar ett nätverk?
5. Hur fungerar Cisco ISE?
6. https://www.cisco.com/c/en/us/products/security/index.html

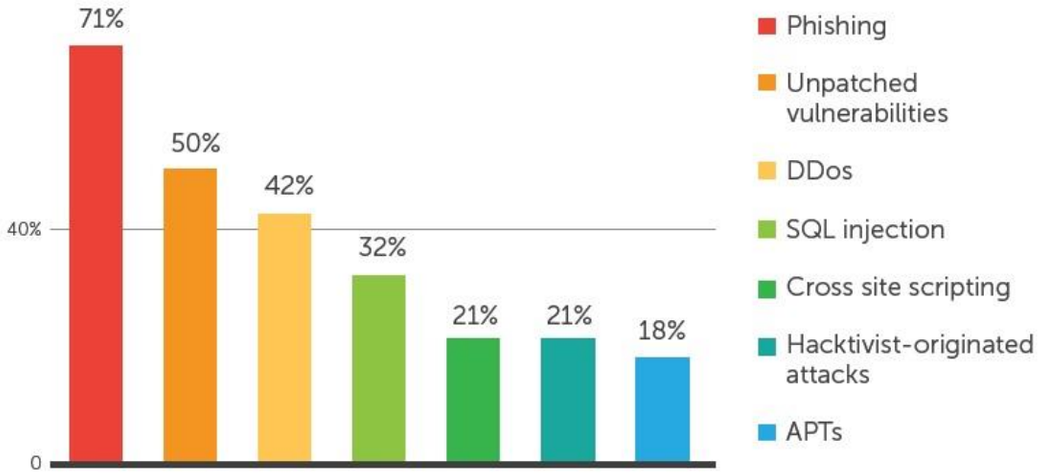
Inledning till cybersäkerhet

1. Keith Barker leder oss inne i cybersäkerhet.
2. Han förklarar konceptet och tar upp nya begrepp.
3. https://www.youtube.com/watch?v=ULGILG-ZhO0



Attackvektorer

- Metoder som angripare använder för att komma åt målet.
- Stegen som angripare följer i sitt attack, en egen strategi.
- Som exempel visar diagrammet nedan de viktigaste typerna av attackvektorer riktad till industriella nätverk:
- Vilka utför attacker mot industriella nätverk?
  - Missnöjda anställda
  - Individer / Små grupper / Hackaktivister
  - Konkurrenter
  - Cyberkriminella grupper
  - Terrorister
  - Religiösa fanatiker
  - Underrättelsetjänster / regeringar



Hacker - hackare

- Skickliga programmerare med kunskap om datorsystem, programmering, nätverk, databas, och datasäkerhet.
- Ethical hacker – identifierar/eliminerar svagheter i ett system
- Cracker – stjälar data, överför pengar till sitt eget bankkonto
- Grey – befinner sig mellan ethical och cracker
- Script kiddies – en som använder befintliga hacker verktyg
- Hacktivist – framför sociala/religiösa/politiska meddelande
- Vulnerability Brokers –
- Cyber Criminals –
- State-Sponsored hacker -

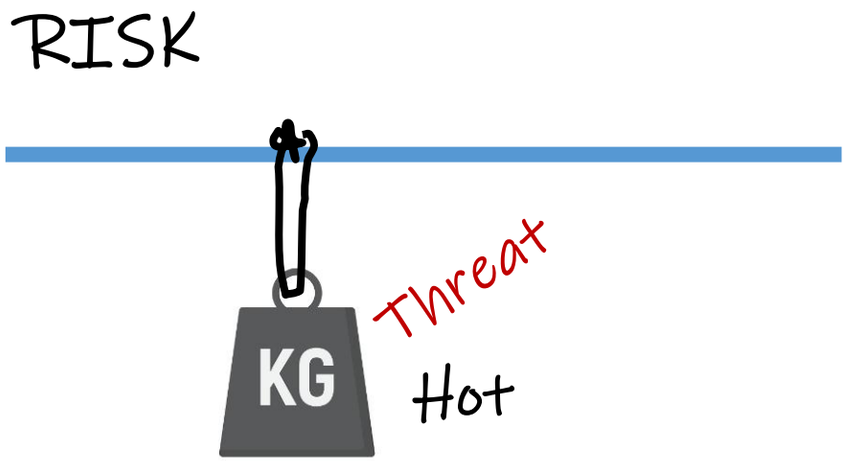
Nätverkssäkerhet

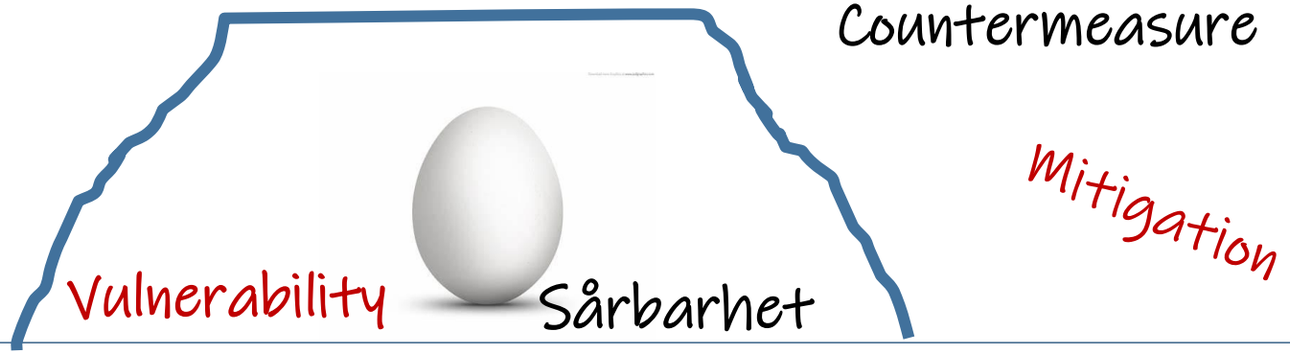
Begrepp inom nätverkssäkerhet

- Threat map
- Vulnerability
- Mitigation
- Risk, risk assessment
- Phishing
- Malware
- Exploit
- Code injection
- DoS
- Social engineering
- APT Advanced Persistent threat
- Zero-Day Exploit
- Integrity
- Countmeassure
- Cookies

Vulnerability - Sårbarhet

- Automatiserade sårbarhetsscanningar identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer.
- Sårbarhetsscanningar:
  - autentiserad och icke-autentiserad
  - Testar säkerhetskontroller
  - Identifierar sårbarheter
  - Identifierar felaktiga konfigurationer
  - Behörig och obehörig åtkomst
- Penetration testning:
  - Verifiera om hot existerar (RISK)
  - Testar säkerhetskontroller
  - Utnyttjande av identifierade sårbarheter
- Penetrationstestrapport inkluderar konkreta slutsatser, tydliga och precisa rekommendationer.





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.

Social Engineering – Social manipulation

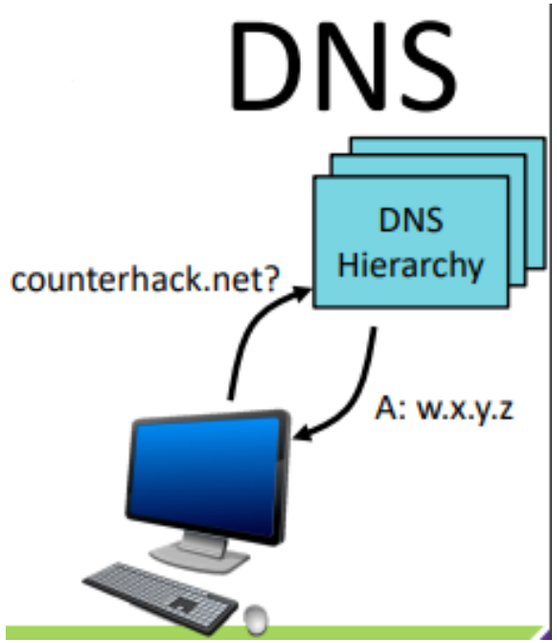
- Social Engineering, eller social ingenjörskonst på svenska, handlar om att manipulera människor så att de lämnar ifrån sig konfidentiell information.
- De som ägnar sig åt Social Engineering utger sig ofta för att vara en person med hög befogenhet som befinner sig i en tidspressad situation.
- Genom 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.

Malware – skadlig programvara

- Termen *"malware"* är en kombination av orden *"malicious"* och *"software"* och är program som kriminella har skrivit i syfte att infektera datorer och andra enheter.
- 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 avancerad skadlig program som undviker detektorer, komprimerar och krypterar filer.
  - **Trojaner**
  - **Spyware**
  - **Maskar**
  - **Ransomware**
  - **Adware**
  - **Scareware**
  - **Packed**

DNS Name System Mischief

- Attackers har utnyttjat en ”bajillion” identiteter.
- De loggar in som kunder hos infrastrukturleverantörer
- Ändrar DNS-poster för att peka på onda webb- och postservrar.
- Angripare samlar e-post …
- Och registrerar sig för ett TLS-certifikat från Comodo
- Och de aldrig tar paus!
- Utmärkt rapportering av Cisco Talos (DNSpionage), FireEye, CrowdStrike och Brian Krebs



Cookies

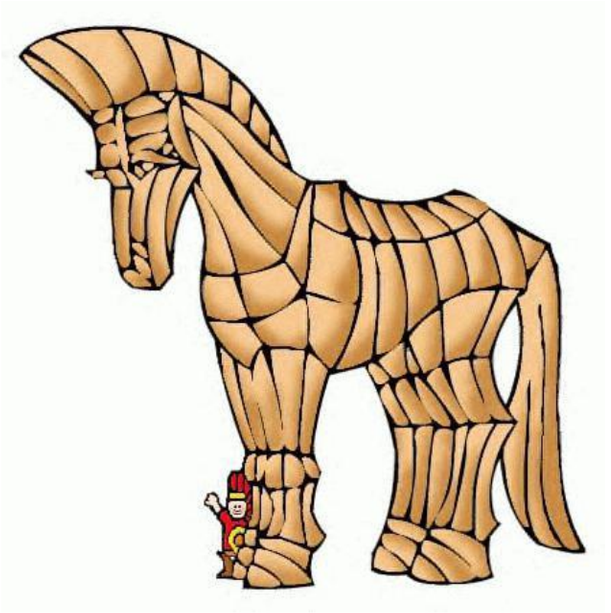
- Cookies är textbaserade små filer som sparas ner i din dators minne när du är inne på en hemsida.
- Det finns två olika typer av cookies.
- Den ena typen sparas i din hårddisk under en längre tidperiod.
- Dessa cookies kommer med ett visst utgångsdatum och när det datumet har passerats så raderas de automatiskt från din dators minne.
- Den andra sortens kallas för *sessioncookies* som raderas när du stänger ner din webbläsare.

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

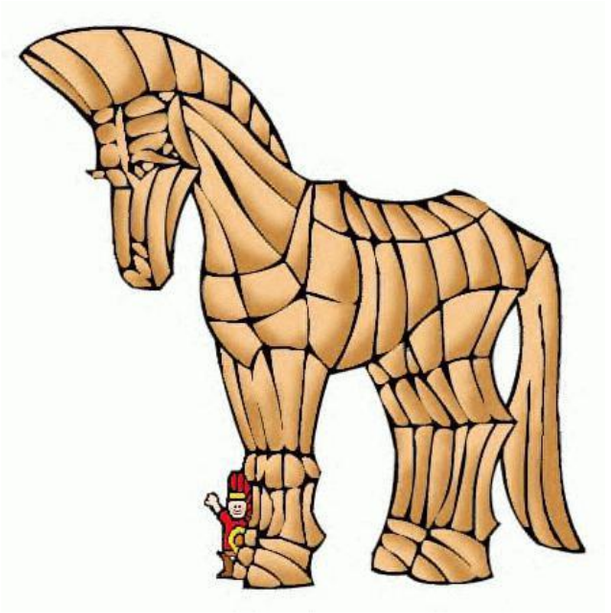
Typer av trojaner

- *Bakdörr* - fjärrkontroll över den smittade datorn, används ofta för att skapa ett botnät eller zombie-nätverk.
- *Kryphålsprogram* - utnyttjar en sårbarhet i ett program.
- *Rootkit* - Rootkits kan hindra att skadlig programvara upptäcks.
- *Banktrojan* - Banktrojaner har utformats för att stjäla kontoinformationen till ditt bankkonto online, e-betalningssystem och kredit- och kontokort.
- *DDoS-trojaner* - utför överbelastningsattacker.
- *Filhämtande trojaner* - kan hämta och installera nya versioner av skadliga program på datorn, till exempel annonsprogram.



Typer av trojaner

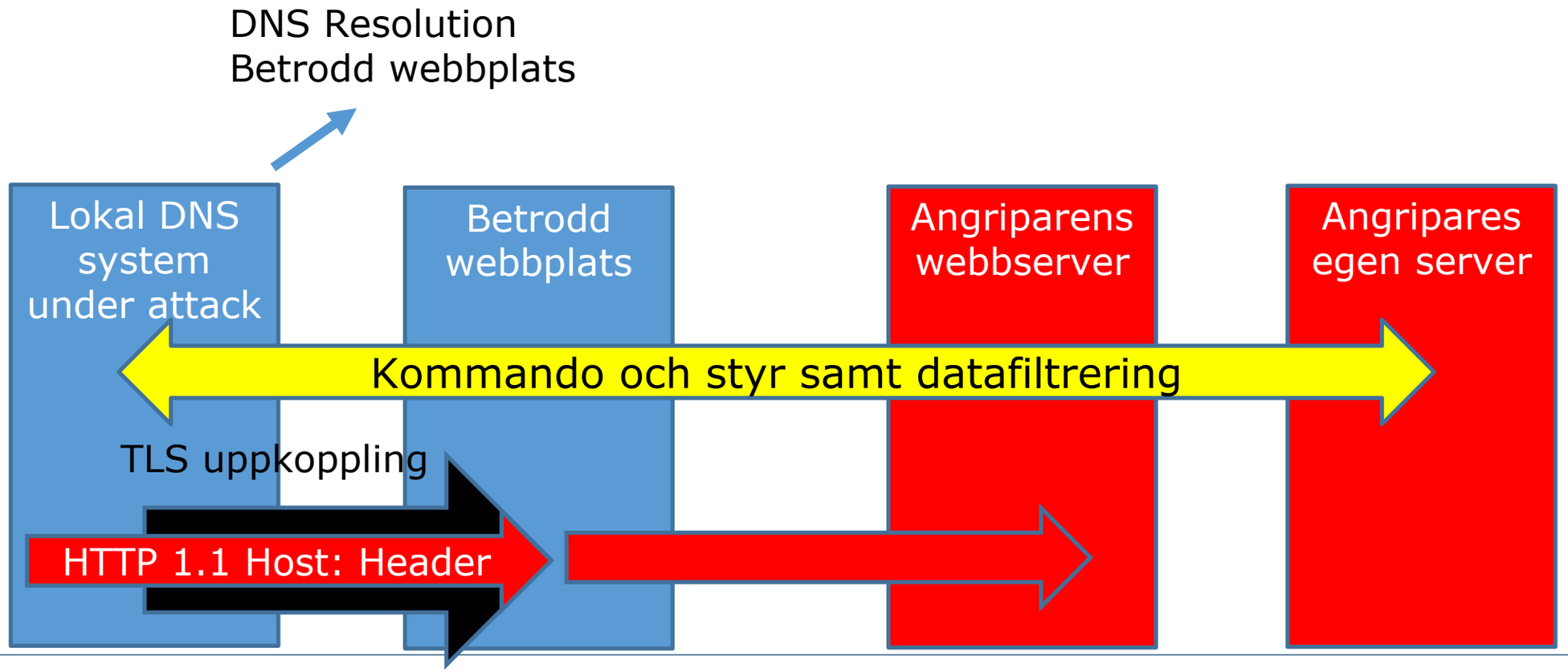
- *Nätverksspelstrojaner* - stjäl användares kontoinformation.
- *Utpressningstrojaner* - återställer din dators funktion eller låser upp dina data enbart efter att du har betalat den lösensumma de kräver.
- *SMS-trojaner* - De här programmen kan kosta pengar för dig genom att de skickar textmeddelanden från din mobila enhet till betaltelefonnummer.
- *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 troligt många andra kriminella handlingar.



Nätverkssäkerhet

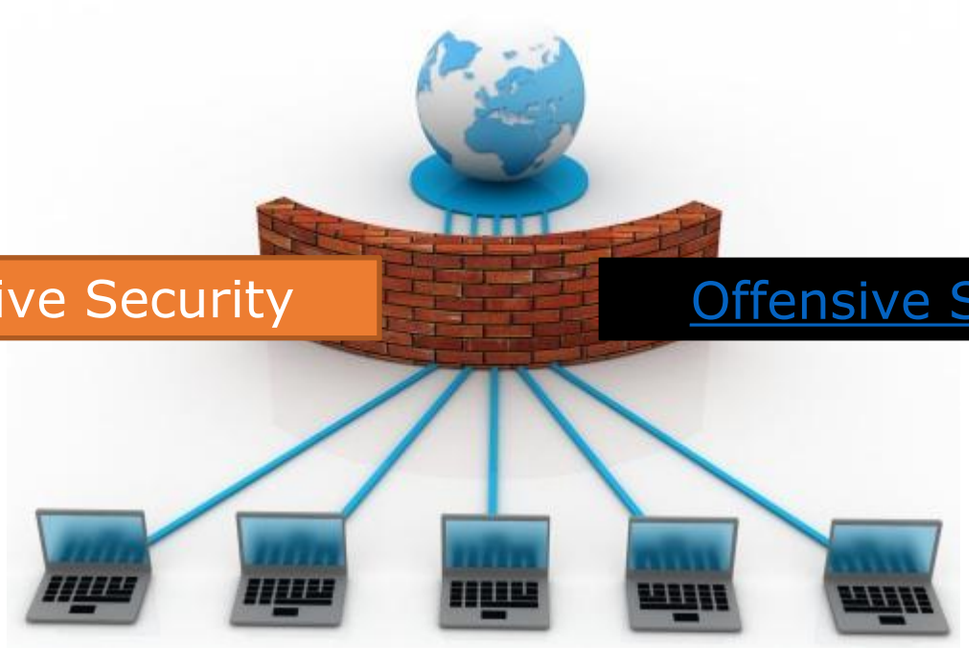
Domän fronten

- Vissa tycker att detta är svårt för angripare ... det är faktiskt inte!
- Vissa tror att det här är säkrad ... det är faktiskt inte!
- DNS är mycket användbart för angripare som försöker dölja kommandokontroll- och kontrollkanaler och filtrera bort komprometterade data.



Att skydda ett nätverk

- Defensiv eller offensiv försvarsteknik?
- Defensiv säkerhet – Försvarsteknik t e antivirus, antimalware
- Offensiv säkerhet – simulering av hack-attacker så att man kan attackera tillbaka, men betraktas som cyber-brott.



Defensive Security

Offensive Security

IINS - Cisco

CCSP - Cisco

CCIE- Cisco

Ethical Hackning

WAPT

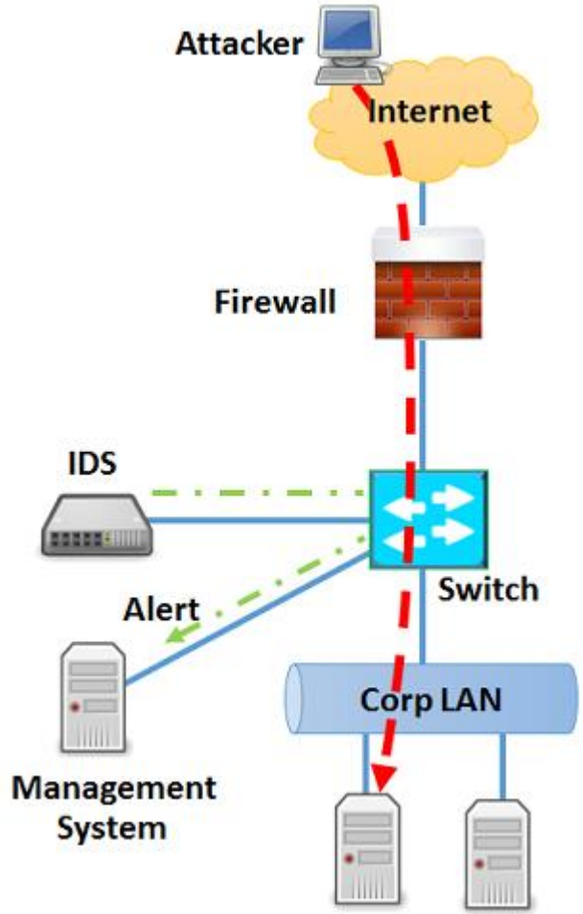
others

Att skydda nätverket

- Nätverkssäkerheten är det primära ansvaret för alla nätverksanvändare.
- Användare bör utbildas kring alla möjliga nätverkssäkerhetsfrågor.
- Interna hot
- Organisationernas personal har oftast direkt tillgång till nätverksresurser och kanske kunskap om företagets nätverks uppbyggande och fungerande.
- En missnöjd anställd kan utnyttja behörigheter och gällande protokoll med syfte att påverka nätverkets infrastruktur eller komma åt hemlig information.

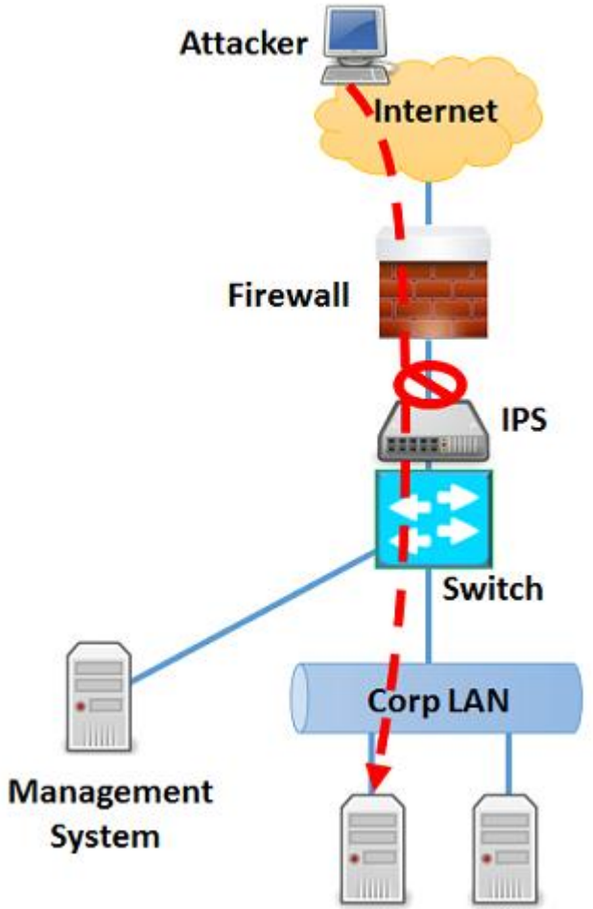
Att skydda nätverket

- Intrusion Detection System – intrångsdetekteringssystem 1984
- Övervakar all inkommande och utgående nätverksaktivitet och identifierar eventuella misstänkta attackmönster.
- Nätverkssäkerhetsspecialister kan minska effekterna.
- Ett passivt övervakningssystem som detekterar och varnar vid misstänkta aktivitet.
- Från billiga shareware eller fritt distribuerade program till en mycket dyrare och säker leverantörsprogramvara.
- Från programvaror och hårdvaruapparater till sensorer på strategiska platser.



Att skydda nätverket – IPS 1998

- IPS upptäcker skadlig aktivitet och automatiskt blockerar det.
- IPS tillhandahåller säkerhet från OS till datapaket.
  - Signaturbaserad detektion
  - Anomalibaserad detektion
  - Reputation-baserad detektion
- För närvarande finns det två typer av IPS:
  - host-baserade HIPS
  - nätverksbaserade NIPS
- IDS och IPS kan implementeras i Cisco IOS
- Skillnader mellan IDS och IPS
  - IDS informerar om en eventuell attack
  - IPS kan stoppa den.

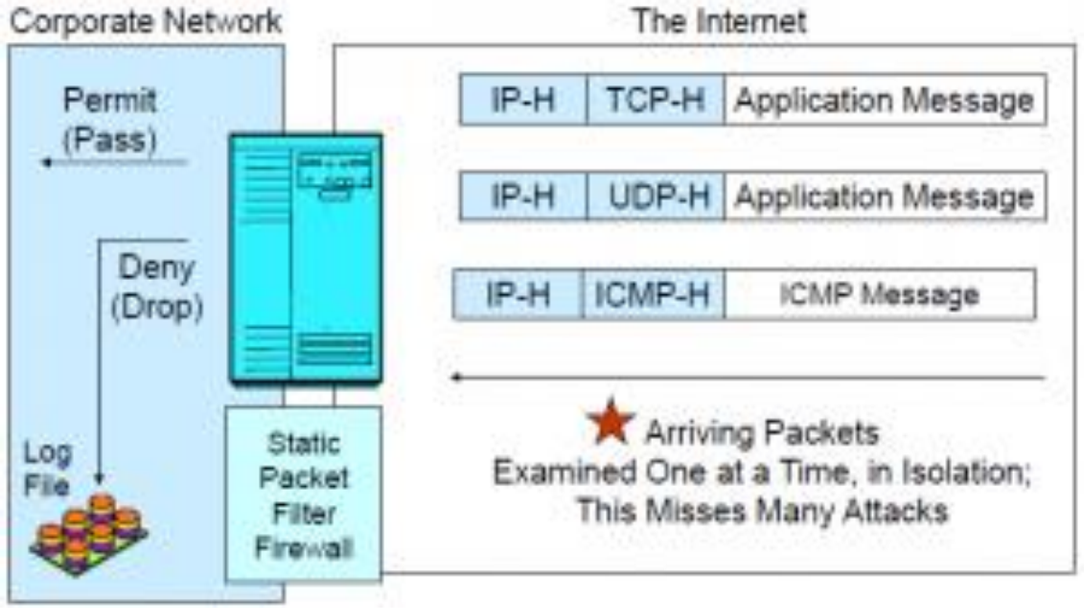


Att skydda nätverket

- Keith Barker förklarar skillnaden mellan IDS och IPS samt två olika implementationer.
- Det ger också fördelar och nackdelar.

Utveckling i nätverkssäkerhet

- 1988, Digital Equipment Corporation (DEC) skapade den första nätverks brandvägg i form av ett paketfilter.
- Dessa tidiga brandväggar inspekterade paket för att se om styrinformation i paketen matchade fördefinierade regler.
- Beroende på kontrollmekanismers resultat kunde brandväggar ta beslutet om att vidarebefordra eller ta paketen bort från nätet.

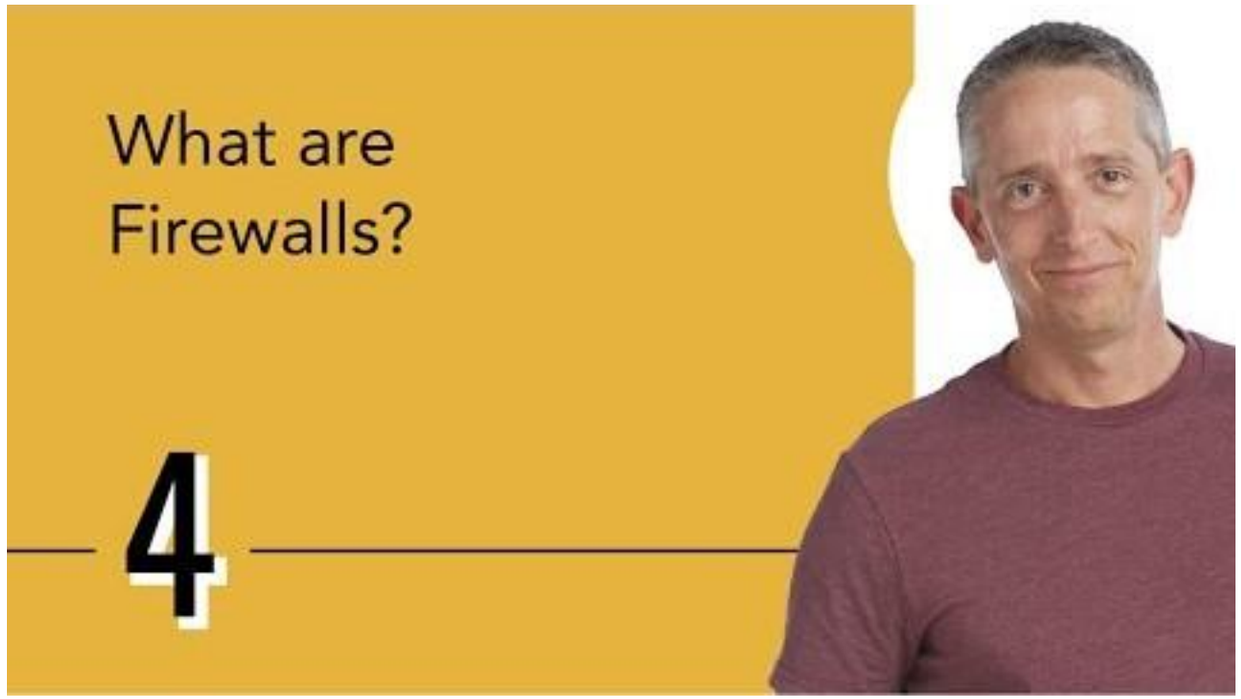


Dedikerade brandväggar

- Avlastar routrars brandväggsfunktioner.
- Brandväggsfunktioner baserade på flera filter.
- Hoten blev mer sofistikerade därmed filter inte tillräckliga.
- Det krävs effektiva försvarsmekanismer som larmar direkt intrång.
- Av denna anledning utvecklade Cisco Security Intelligence Operations (SIO) ASA brandvägg.
- SIO är en molnbaserad tjänst som identifierar globala hot och samlar information kring deras beteende.
- ISA 3000
- Industrial Security Appliance

Dedikerade brandväggar

- Vad är brandväggar?
- Keith Barker besvarar frågan och förklarar några termer som förklaras av Keith Barker:
- Rules and exceptions
- Trusted network and Untrusted network
- DLP – Data Loss Prevention
- NGFW – New Generation FW
- UTM – Unified Threat Management
- IPS/IDS
- URL filtering



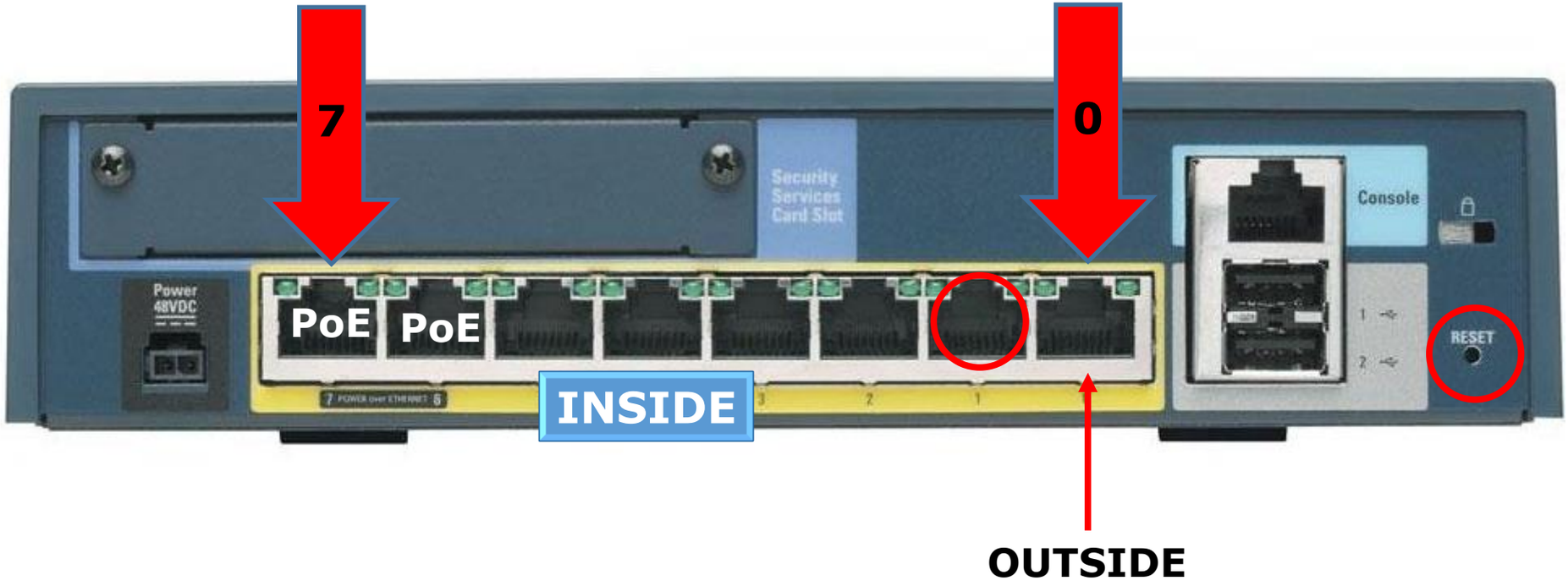
Nätverkssäkerhet

Cisco ASA 5505

- Cisco ASA 5505 är en relativ liten men stark brandvägg.
- Cisco ASA 5500-serien erbjuder intelligent försvar som stoppar attacker innan de tränger in i nätverksgränser, kontrollerar nätverks- och applikationsaktivitet och ger säker fjärråtkomst och anslutning.
- Cisco ASA 5505 stödjer SSL och IPsec VPN
- Med hjälp av den integrerade Cisco ASDM kan Cisco ASA 5505 konfigurationer snabbt distribueras och enkelt hanteras.
- Cisco ASA 5505 har 8-port 10/100 Fast Ethernet-switch, vars portar kan dynamiskt grupperas för att skapa upp till tre separata VLAN.
- Cisco ASA 5505 tillhandahåller två Power over Ethernet (PoE) –portar.

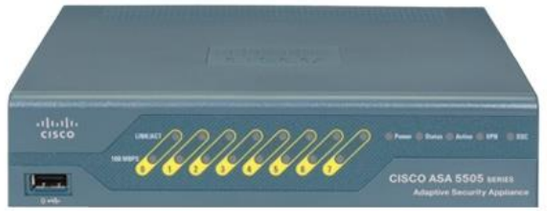
Cisco ASA 5505

- Denna brandvägg har 8 Ethernet portar numrerade från höger till vänster.
- Säkerhetsnivåer: Hög = Inside 100 och LÅG = Outside 0
- Säkerhetskonfigurationer kan kombineras med NAT och ACL
- På insidan körs en lokal DHCP server.



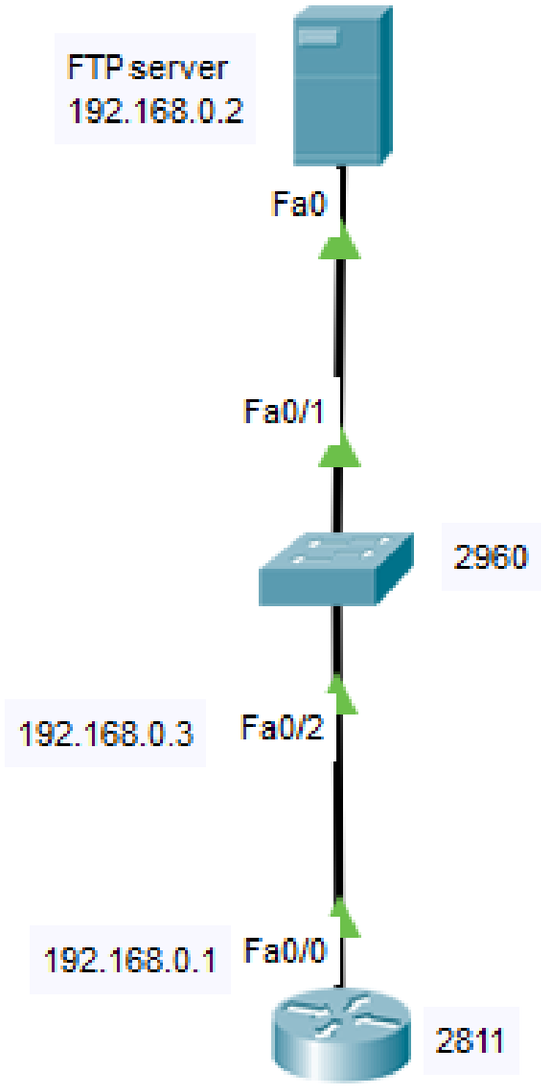
Brandväggfunktioner i Packet Tracer

- Det kräver IOS version 15 på vissa Cisco routrar för att få brandväggfunktioner.
- Cisco IOS-nätverkshanterare såsom switchar och routrar använder vanligtvis sitt flashminne för att lagra IOS-image.
- På de flesta routrar kan detta flashminne enkelt bytas ut.
- Men på vissa switchar är flashminnet integrerat i moderkortet och det kan inte bytas ut.
- Steg 1: Välj en **Cisco IOS** Image. ...
- Steg 2: Ladda ned **Cisco IOS** Image till TFTP Server. ...
- Steg 3: Identifiera filsystemet ditt IOS-image ska kopieras.
- Steg 4: Förberedd uppgraderingen
- Steg 5: Verifiera kommunikationen mellan router/switch och TFTP server
- Ste6 6: Kopiera IOS image till router/switch



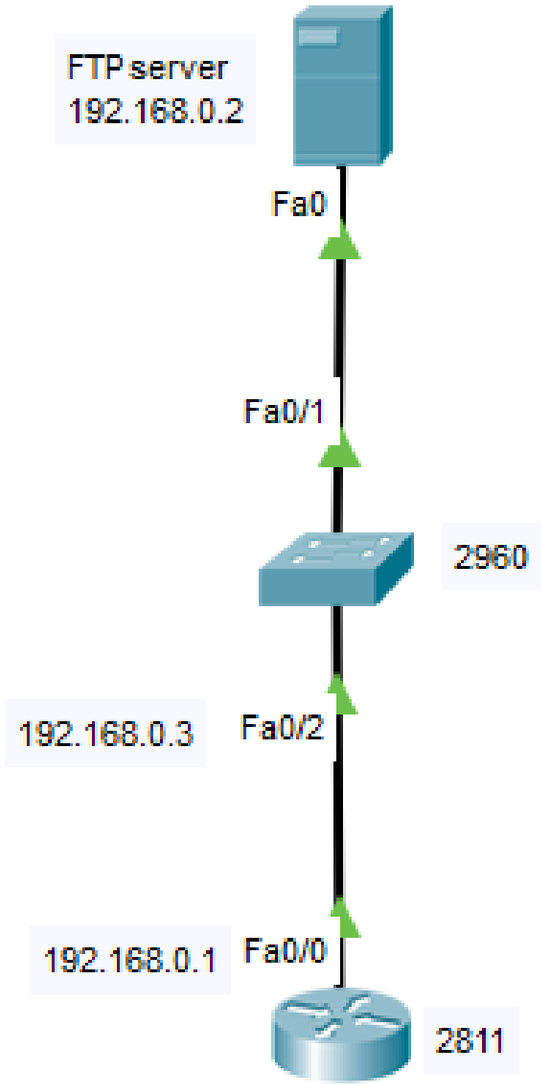
Demo: Uppgradera cisco IOS

- En TFTP server, en 2960 switch och en router 2811
- Switch# dir
- Från: c2960-lanbase-mz.122-25.FX.bin
- Till: C2960-lanbasek9-mz.150-2.se4.bin
- Router# show version
- Från: c2800nm-advipservicesk9-mz.124-15.T1.bin
- Till: C2800NM-ADVIPSERVICESK9-MZ.151-4.M4.bin
- Konfigurera FTP server där finns som default användarkonto: cisco lösenord: cisco
- Enklare om man använder TFPT server som inte kräver autentiseringsuppgifter.



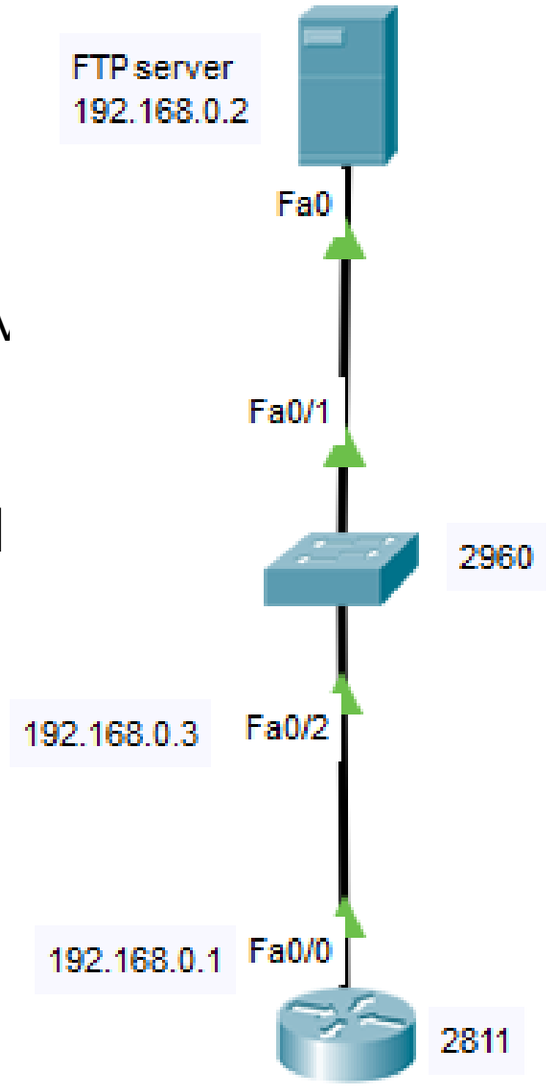
Demo: Uppgradera cisco IOS

- Switch(config)# int vlan 1
- Switch(config-if)# ip address 192.168.0.3 255.255.255.0
- Switch(config-if)# no shut
- Switch(config-if)# exit
- Switch(config)# ip default-gateway 192.168.0.1
- !
- Router(config)# int fa0/0
- Router(config-if)# ip address 192.168.0.1 255.255.255.0
- Router(config-if)# no shut



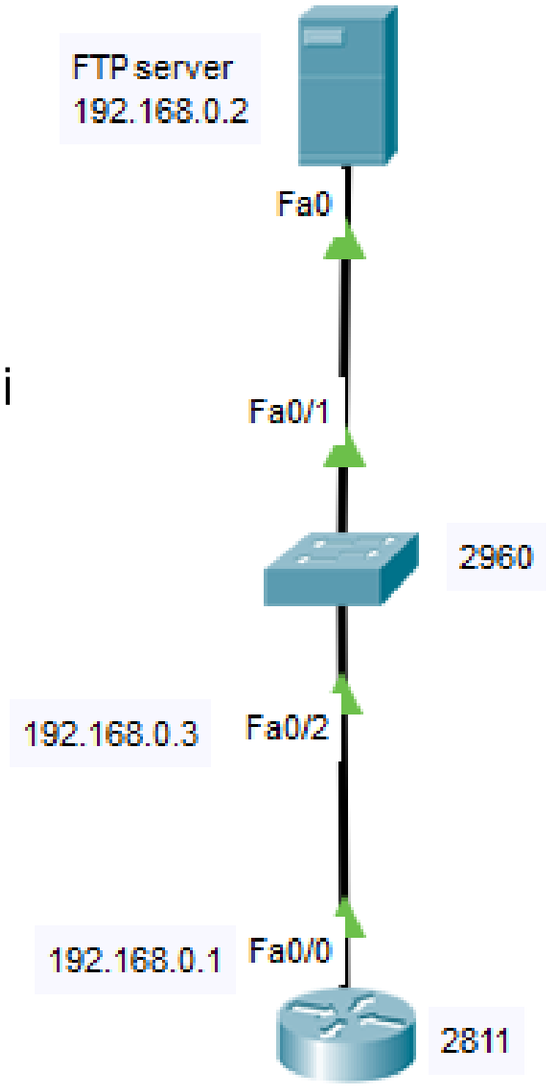
Demo: Uppgradera cisco IOS

- Router# dir – eller – dir flash:
- Oftast behöver man rensa flash-minnet först!
- Router# copy tftp: flash:
  - Address or name of remote host []? 192.168.0.2
  - Source filename []? c2800nm-advipservicesk9-mz.151-4.M4.bin
  - Destination filename [c2800nm-advipservicesk9-mz.151-4.M4.bin]? (
- Router# delete c2800nm-advipservicesk9-mz.124-15.T1.bin
  - Delete filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?
  - Delete flash:/ c2800nm-advipservicesk9-mz.124-15.T1.bin? [confirm]
- Router# copy tftp: flash:
  - Address or name of remote host []? 192.168.0.2
  - Source filename []? c2800nm-advipservicesk9-mz.151-4.M4.bin
  - Destination filename [c2800nm-advipservicesk9-mz.151-4.M4.bin]?



Demo: Uppgradera cisco IOS

- Switch# dir – eller – dir flash:
- Switch# copy tftp: flash:
  - Address or name of remote host []? 192.168.0.2
  - Source filename []? C2960-lanbasek9-mz.150-2.se4.bin
  - Destination filename [C2960-lanbasek9-mz.150-2.se4.bin]?
  - Kopieringen startar bra men i slutet misslyckas.
- Switch(config)# boot system C2960-lanbasek9-mz.150-2.se4.bi
- Switch(config)# exit
- Switch# write
- Switch# reload




DIGINTO
Nätverkssäkerhet