Understanding Firewalls

Hva en som skal angripe systemet tenker på:

- ⇒ Hva er det jeg skal oppnå med angrepet?
- ⇒ Hvilke svakheter/sårbarheter finnes og hvilke kan utnyttes?
- ⇒ Hvilken skade eller andre konsekvenser er sannsynlige?
- ⇒ Hvilke utnyttelser eller andre angrepsverktøy er tilgjengelige?
- ⇒ Hva er risikoen for at jeg blir oppdaget eller tatt på fersken?

Internet traffic must be routed to the correct place directly, and online data must know where its going. How does the information know where it's supposed to go? This is where TCP/IP comes in. That stands for: Transmission Control Protocol and Internet Protocol. You can think of it as a sandwich because its conceptionalized in layers.

The top layer is called Application Layer. Which is like what programs our web browser directly interacts with. This layer har protocol like HTTP if youre visiting websites or SMTP if youre checking your email.

The next layer is the Transport layer. Where TCP lives with another scheme called UDP, which is a bit faster for low latency applications like online games. After the application layer gets the data from whatever program you are using, it talks to the transport layer through something called a port. Each port can be assigned to a different protocol in the application layer so the TCP knows where the data is coming from. For example most web browser acitivty will go through port 80 which is what HTTP always uses.

Once TCP gets the data it chops it up into small chunks called packets. They can individually take the quickest route over the internet to get to where they are going. TCP slaps a header into each packet that contains instructions in what order to assemble the packets into as well as some information that can help the receiver computer understand if the data has arrived in its original state.

After this is done the packets are pushed into the internet layer, which uses the internet protocol or IP to attach both the origin and the destination IP addresses so the packet knows where it came from and where it's going. The data is then sent through the final network layer that handles things like MAC addressing, so the packets go to the right physical address in the right machine as well as converting the data into electrical impulses that will actually pass through the proverbial series of tubes.

Although every single packet has to go through each layer, packet switching makes the internet faster than it would otherwise be, since it allows each packet to individually to avoid congestion and bottlenecks that would occur if all data had to take the same route.

STEPS OF AN ATTACK

1. Utforsking
    - Innhenting av informasjon som er offentlig tilgjengelig
        1. WHOIS- og DNS-forespørsler
        2. Offerets nettside (Informasjon om brukere/brukernavn). Nyttig for sosial manipulasjon.
        3. Noen selskaper oppgir informasjon om teknologiene de bruker på sine nettsider.
2. Rekognosering
    - Kartlegging av nettverket (Fastslå om systemet er aktivt)
        1. Identifisering av tilkoblede og aktive maskiner i nettverket
    - Portskanning
        1. Identifisering av åpne porter på systemet
    - Fingerprinting
        1. Identifisering av type serverapplikasjon, versjon og OS-versjon
3. Gjennomføre angrepet
    - Lokalisering/Søk etter potensielle sikkerhetshull og sårbarheter for den spesifikke serverapplikasjonen/OS-en og utføre angrepet
4. Lateral bevegelse
    - Når angrepet lykkes, eskalere privilegier
5. Opprettholde tilstede

- Opprette bakdører for fremtidig bruk

PORT-SCANNING

- Et program som systematisk skanner alle nettverksporter på en datamaskin for å finne informasjon om datamaskinens tjenester.
- Nmap tilbyr flere ulike teknikker for å finne informasjon.
- Det er ulovlig i noen deler av verden å utføre portskanning. Det viktige når du bruker portskanningverktøy er å sørge for at du er innenfor et nettverk hvor du har tillatelse til å utføre portskanning!

VANLIGE NMAP OPSJONER

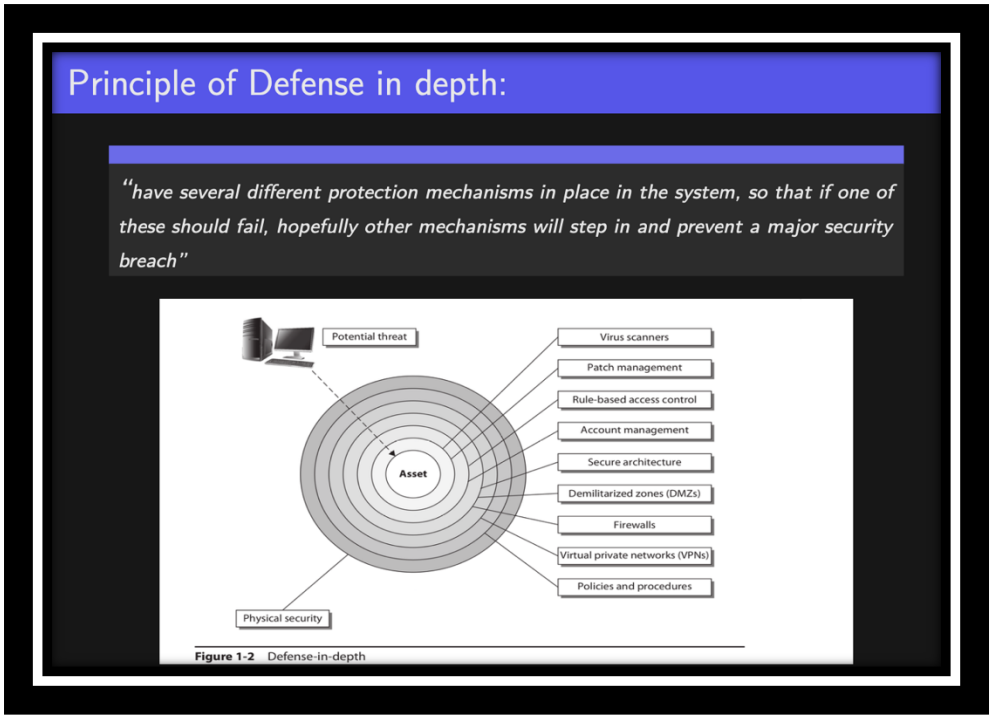
- -sS TCP SYN scan
- -sT TCP connect() scan
- -sU UDP port scans
- -O Detect Operating System (TCP/IP fingerprinting) I -sV Service version detection
- -PN Don’t ping, just scan
- -A Aggressive Options
- -T Paranoid|Sneaky|Polite|Normal|Aggressive|Insane
- -p Choose your ports (scan all ports with 0-65535)
- -F Fast Scan:Scans only ports in the nmap-services file I -n Don’t do reverse DNS lookup
- -v Verbose output
- -vv Very verbose output

HVORDAN KAN VI FORHINDRE PORT-SCANNING?

I praksis er det ofte svært vanskelig å skille mellom legitim trafikk og uønsket trafikk. Vi kan bruke brannmurer for å blokkere porter. Vi kan bruke innbruddsdeteksjonssystemer som har innebygde mekanismer for å oppdage portskanning. Dette kan imidlertid ofte føre til mye unødvendig trafikk (falske positiver), noe som kan føre til at funksjonaliteten slås av!

TRENGSEL FOR BRANNBURER?

Mens internett-tilgang gir fordeler for organisasjonen, gir det også mulighet for at omverdenen kan nå og samhandle med lokale nettverksressurser. Dette utgjør en trussel for organisasjonen.



HVA ER EN BRANNMUR?

- Et nettverkspunkt som lar oss kontrollere og overvåke nettverkstrafikken
- En brannmur kontrollerer tilgang til/fra nettverket/maskinen basert på sett med regler
- Den pålegger begrensninger på nettverkstjenester og nettverkstilgang
    - Bare autorisert trafikk tillates

BRANNMUR KRAV

1. All trafikk/kommunikasjon mellom "ekstern" og "intern" må passere gjennom brannmuren.
    1. "Intern" og "ekstern" blir ofte definert med ulike nivåer av tillit.
2. Kun autorisert trafikk bør tillates å passere.
    1. "Autorisert trafikk" blir definert av lokal sikkerhets-/brannmurpolicy.
3. Brannmuren selv bør ideelt sett være godt beskyttet mot angrep.
    1. Programvare har ofte feil og sårbarheter.

BRANNMUR POLICY

1. Identifisere tjenester
    - Hvilke tjenester kan få tilgang fra internett til det lokale nettverket?
    - Typiske tjenester inkluderer HTTP, HTTPS, SMTP, DNS, SSH, VPN, osv.
2. Avgjøre tilgjengelige tjenester
    - Hvilke tjenester på internett kan maskinene i det lokale nettverket tillates å få tilgang til?
    - Er det tillatt med peer-to-peer musikk- og filnedlasting?
3. Definere standardpolicy
    - Blokkere all trafikk og tillate etter behov
    - Tillate all trafikk og blokkere etter behov

DEFINER STANDARD POLICY

The firewall must have a policy on how to handle a package:

- Accept it
- Drop it (silently discard it)
- Reject it (discard and send ICMP notification)
- Logit Change header information (e.g. NAT)

ULIKE TYPER FIREWALL

Pakkefilter (Stateless)

- Enkelt, statisk
- Kontrollerer tilgang basert på
    - Avsender/mottaker IP-adresse
    - Avsender/mottaker portnummer

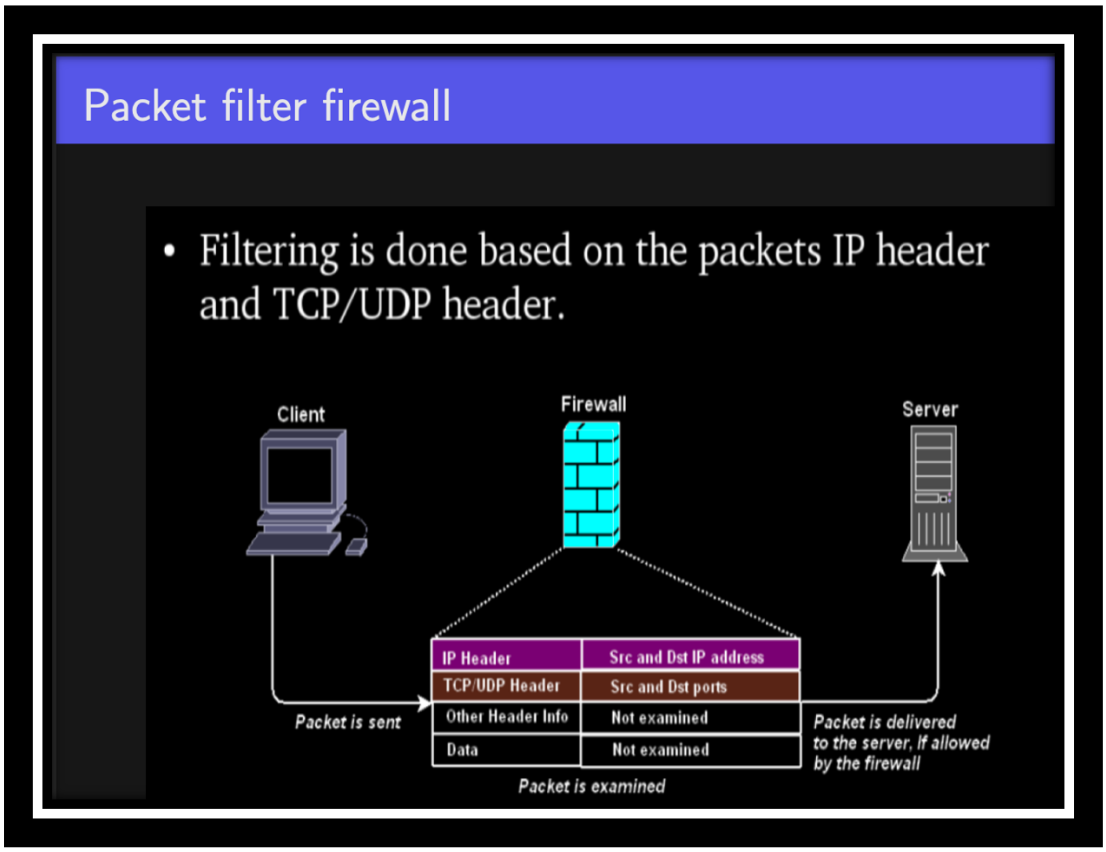
Dynamisk pakkefilter (Stateful brannmur)

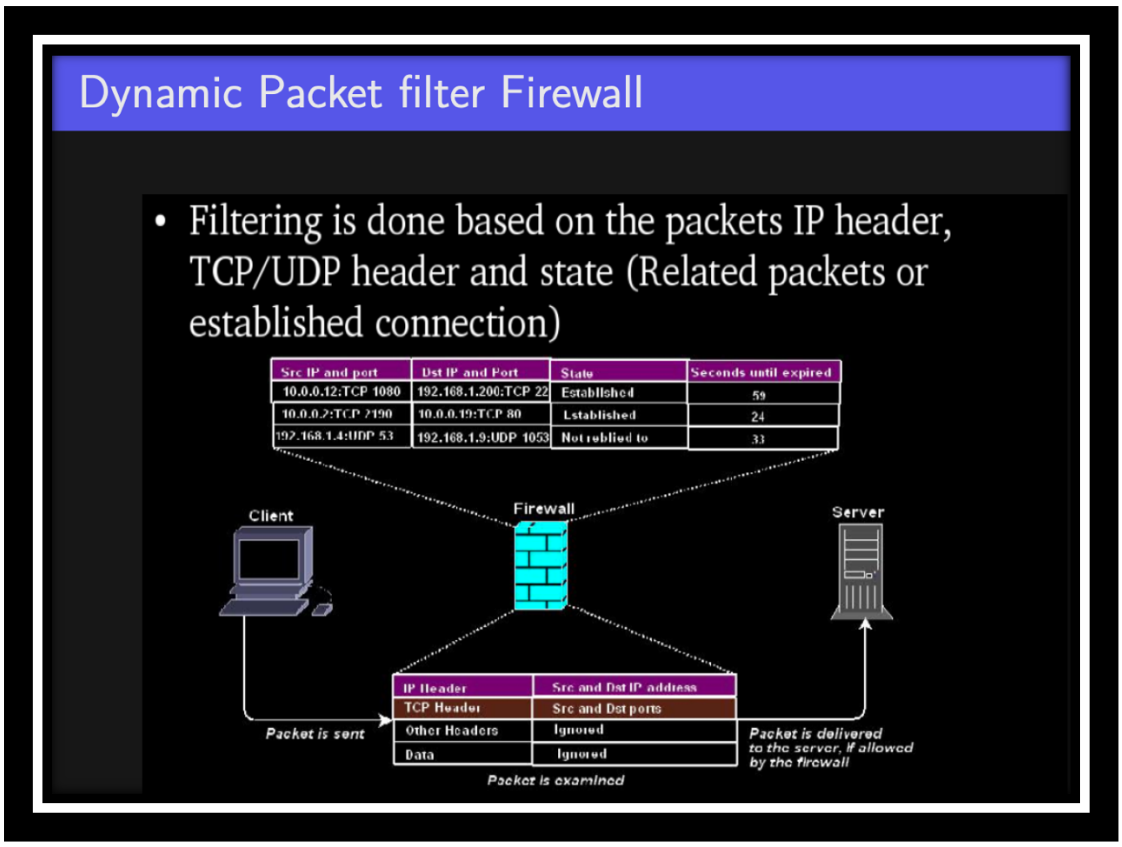
- Opprettholder "tilstandsinformasjon" fra en pakke til den neste
- Holder styr på sekvensnumre og forhold til påfølgende pakker

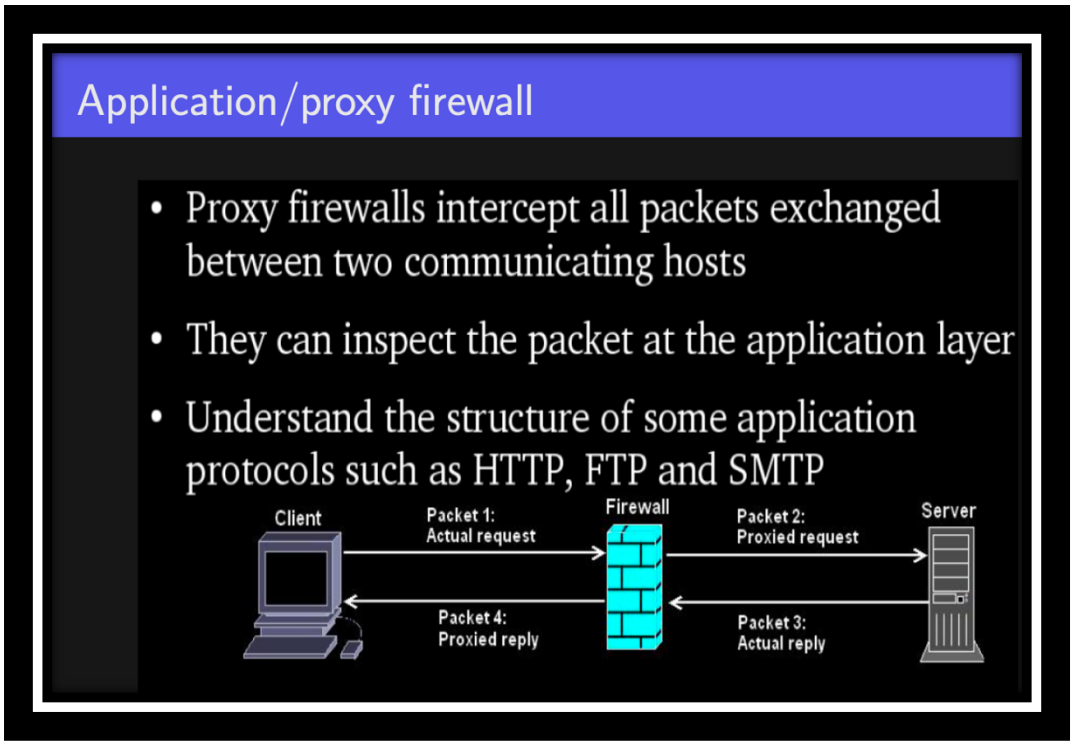
Applikasjon/proksy-brannmur

- Ser på hver pakke lag for lag og setter dem sammen igjen før de sendes ut
- Holder styr på sekvensnumre og forhold til påfølgende pakker
- Kommunikasjon gjennom brannmuren/proksyen er delt inn i to
    - Avsenderen på utsiden ser brannmuren som mottakeren

- Mottakeren på innsiden ser brannmuren som avsenderen







BRANNMUR BEGRENSNINGER

- Gir ikke beskyttelse mot trafikk som omgår brannmuren
  - Dvs. fysiske inntrengere, bruk av modem/3G/4G, betrodde organisasjoner, betrodde tjenester (HTTP, HTTPS, SSH, SMTP, IMAP eller VPN)
- Gir ikke beskyttelse mot interne trusler (insidere)
  - Dvs. illojale ansatte med ondsinnet hensikt
- Gir ikke beskyttelse mot overføring av virusinfiserte programmer, filer, trojanere eller phishing-svindel.

BRANNMUR ARKITEKTUR

- Personlig/enkeltstående
  - Filtrer innkommende og utgående trafikk på en enkelt datamaskin
- Bastion
  - En enkel brannmur som står mellom det lokale nettverket og internett
- Skjermet vert
  - Brannmuren i skjermet vert-arkitekturen kommuniserer med en ruter som først filtrerer all ekstern trafikk
- Skjermet delnett
  - I skjermet delnett brukes to brannmurer, og nettverket er delt inn i to soner

- En sone kalt Demilitarisert Sone (DMZ), som er eksponert for ekstern trafikk og beskyttet av den første brannmuren
- En intern sone som ikke er eksponert for ekstern trafikk og som beskyttes av den andre brannmuren