**Week-06 Network/network protocols and Security**

For all questions below, use stored Wireshark samples to support your answer

**Agenda:**

1. Forklar TCP/IP protocol stack og de protokoller der indgår i hvert lag.
2. Forklar TCP ”Three-way handshake”, og vis eksempel på hvordan en hacker kan udnytte dette
3. Forklar om DNS systemet og vis eksempel på hvordan en hacker kan udnytte dette.
4. Forklar om DHCP protokollen og vis eksempel på hvordan en hacker kan udnytte dette.

**Explain conceptually the purpose of the layers in the TCP/IP protocol stack**

**Explain conceptually the TCP/IP protocols involved in transporting a package (HTTP for example) from Source to Destination.**

Transmission Control Protocol/ Internet Protocol. TCP/IP er en række protokoller, der anvendes til at forbinde hosts (computer tilgået af en bruger) over internettet. TCP/IP er standardprotokollen til at transmitte (udsende) data over netværker. TCP og IP er de primære protokoller

TCP/IP protocol Stack består af fire lag:

1. **Application** - Dataenhed: Data (Den del som brugerne interagerer med eksempelvis en fil (ftp), webbrowser (http) eller email (smtp) applikation som outlook).

Grænsefladen mellem en applikationslags protokol og en transportlags protokol er defineret med henvisning til portnummer.

Vi har sendt et GET request, og fået data tilbage, som text/html.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

Data der sendes over http, vil som oftest bestå af head og body.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

1. **Transport** - Dataenhed: Segmenter (Gennem TCP kan programmer på forskellige hosts på internettet oprette forbindelser mellem hinanden, der kan udveksles data pakker)

Eksempel: TCP er det bedst kendte eksempel på transportlaget, TCP opdeler dataen i segmenter. Hvert segment har et kilde- og destinationsportnummer (til og fra), samt et sekvensnummer. Portnummeret sikrer, at segmentet når den rigtige applikation. Sekvensnummeret sikrer, at segmenterne ankommer i den rigtige rækkefølge, da segmenterne bliver overført individuelt på den hurtigste måde, over forskellige dataveje.

Dette lag håndterer også fejlhåndtering. Hvis et segment skulle mangle sørge dette lag for at retransmittere det manglende datasegment.

Det er i dette her lag, at kilde- og destinations portnummer kommer på.



Her bliver der afgjort hvilken transport protokol der skal anvendes. I dette her tilfælde er det TCP. Derudover opdeles dataen i mindre pakker. Hver gang en pakke modtages hos klienten, sendes en kvittering tilbage til serveren (som en lille datapakke).

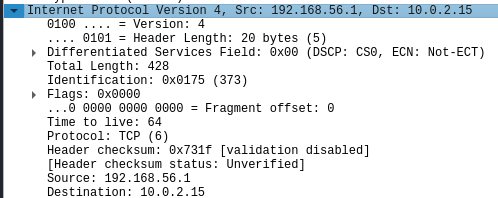
Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse



1. **Networking** (internet) - Dataenhed: Packets (Transmitterer data segmenter mellem netværk i form af packets. Når du sender en besked til din ven, tildeler dette lag kilde- og destinations-IP-adresser til data segmenterne. Din IP-adresse er kilden, og din ven er destinationen. De vigtigste funktioner i dette lag er at tage sig af adressering, montering og demontering af datapakker).

Som det ses på billedet, er der blevet tildelt kilde- og destinations IP-adresser.



1. **Network access (Datalink og fysisk lag)** - Dataenhed: bit og frames

Dette lag modtager packets fra networking og tilføjer afsender- og modtager MAC-adresser til datapakkerne og oversætter disse til frames.

Dette gør det muligt at sende disse frames over lokale medier, såsom kobbertråde, optisk fiber eller luft. Dette lag er en del af din computers software kaldet NIC

Dette lag giver altså de øvrige lag adgang til medier og styrer, hvordan data placeres og modtages fra medier.

Det fysiske lag er det som vi faktisk kan røre (Hardware). Dette lag konverterer det binære fra de øvre lag til signaler og transmitterer dem over lokale medier. Disse kan være elektriske, lette eller radiosignaler; det afhænger af typen af ​​anvendt medie.



**Explain the purpose of the DNS system and the DHCP protocol**

Systemet DNS (Domain Name System) oversætter domænenavne til ip-adresser via DNS servere, dette gælder dog kun for et begrænset antal domæner. Hvis DNS serveren ikke kan finde den tilhørende ip adresse, kan den kontakte andre DNS servere for at få oversat domænenavnet.

Her kan vi se et eksempel på et serverkald til en DNS-server. Vi kan se at den bruger UDP-protokollen. Vi kan se hvilken hjemmeside, samt dens IP-adresse, vi forsøger at tilgå.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

DHCP(Dynamic Host Configuration [Protocol](https://da.wikipedia.org/wiki/Datanetprotokol)) er en netværksprotokol, der gør det muligt for en server automatisk at tildele en IP-adresse til en computer fra et defineret antal numre, der er konfigureret til et givet netværk. DHCP anvendes til at administrere og tildele IP-adresser i et TCP/IP netværk. DHCP serveren lytter på port 67 og står for at tildele IP-adresser til klienter på et netværk

1. IP-adressen frigives
2. Discover: Leder efter en ny IP-adresse
3. Offer: Får tilbudt en IP-adresse (10.0.2.15) fra DHCP
4. Request: Den vil jeg gerne have
5. ACK: acknowledgement.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

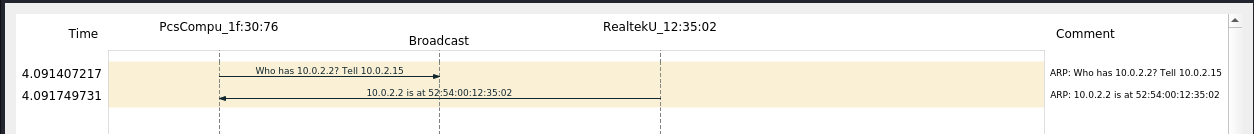
**Explain, conceptually, about the arp-command and the ARP-protocol**

## Arp-kommandoen gør det muligt at se ARP cache, samt at kunne tilføje og slette indhold.

* **ARP** (Address Resolution Protocol) bruges af IP-protokollen i netværkslaget. ARP konverterer IP-adresser til Ethernet adresser (MAC adresser), og ARP protokollen bruges til at opretholde en cache af oversættelser af IP-adresser til MAC adresser.

ARP-protokollen definerer formatet og betydningen af beskeder sendt og modtaget.

ARP er en internetprotokol, som oversætter IP-adresser til MAC adresser (hardware) på et netkort (cache). Protokollen kan kun bruges mellem enheder på samme fysiske net. Når der første gang skal sendes en IP-pakke fra en maskine til en anden, kender afsender maskinen ikke modtageren hardware adresse, og sender derfor en broadcast meddelelse, med den ønskede IP-adresse til alle andre maskiner, på det aktuelle netværk. Den maskine der har den ønskede IP-adresse, sender sin hardware adresse tilbage og gemmer samtidig afsenderens hardware adresse til senere brug.



**Explain conceptually strategies a hacker can use to attack:**

* **The DNS-system**

En hacker kan fra sin egen computer sende request til en DNS-server, som indeholder offerets IP-adresse, som afsender. DNS-serveren vil sende et response til offeret, som vil være 5 gange større, end det request, som hackeren har sendt til DNS-serveren. Hackeren kan altså bruge en DNS-server til at forstærke sit angreb.

For at fungere som man-in-the-middle, skal en hacker lave om i klientens DNS-cache, for på den måde at omdirigere et offer til en falsk hjemmeside, som er en kopi af den side, som vedkommende forsøger at komme ind på. I dette her tilfælde Danske Bank. Forsøger vedkommende at logge ind på sin Danske Bank konto, igennem den falske hjemmeside, kan hackeren få fat på klientens login oplysninger. Vedkommende bliver videreført til den rigtige hjemmeside, og opfatter ikke at en ”man-in-the-middle”, nu har loginoplysningerne.

Et billede, der indeholder skærmbillede, monitor

Automatisk genereret beskrivelse

* **The DHCP protocol**

En hacker kan lukke andre ude af nettet, ved at broadcaste request til DHCP-serveren med spoofed MAC-adresser, til sidst optages alle tilgængelige IP-adresser, og når en rigtig klient vil tildeles en ny IP-adresse, vil klienten lukkes ude af nettet, da DHCP-serveren ikke har flere IP-adresser i sin IP-pool. Dette angreb hedder DHCP-starvation-attack.

Et billede, der indeholder kort

Automatisk genereret beskrivelse

* **The TCP-protocol**

Et ”three-way handshake” er en metode der bruges i TCP/IP netværk til at skabe forbindelse mellem en localhost/klient og en server.

Når serveren modtager en SYN pakke sender den en SYN,ACK tilbage og venter på en ACK. Det kan være relevant for en hacker, der kan lave et SYN FLOOD attack, hvilket vil sige at hackeren sender en stor mængde af SYN pakker til serveren via spoofed IP-adresser. Serveren vil således besvare hver af forbindelses requests med en SYN og ACK, og reserverer derefter en port åben og klar til at modtage en ACK. Mens serveren venter på den sidste ACK, som aldrig bliver modtaget, fortsætter hackeren med at sende flere SYN requests. Hver gang serveren modtager et SYN request vil den reservere en ny port til forbindelse i en hvis mængde tid. Når alle portene så er optaget kan serveren ikke længere fungere normalt. Det er en type af Denail Of Service Attack (DoS).

Et billede, der indeholder computer

Automatisk genereret beskrivelse

* **The ARP-protocol**

ARP-poisoning (også kendt som ARP Spoofing) er en type cyberangreb udført over et Local Area Network (LAN), der involverer afsendelse af ondsindede ARP-pakker til en default-gateway, for at ændre parringen af sin IP og MAC-adresse. ARP-protokol oversætter IP-adresser til MAC-adresser. Da ARP-protokollen udelukkende er designet til effektivitet og ikke for sikkerhed, er ARP- poisoning ekstremt let at udføre, så længe hackeren har kontrol over en maskine inden for netværket.

Selve angrebet består af en hacker, der sender en falsk ARP- reply message til default-gateway, der informerer om, at hackerens MAC-adresse skal være knyttet til offerets IP-adresse (og vice versa, så offerets MAC er nu knyttet til hackerens IP-adresse). Når default-gateway har modtaget denne meddelelse og udsendt dens ændringer til alle andre enheder på netværket, modtager hackeren al offerets trafik til enhver anden enhed på netværket. Dette giver hackeren mulighed for at inspicere eller ændre det, før det videresendes til dets virkelige destination. Da ARP- poisoning forekommer på et så lavt niveau, er brugere, der er målrettet med ARP- poisoning, sjældent klar over, at deres trafik inspiceres eller ændres.

Denne kommando bruges til at videresende til den egentlige destination, så klienten er uvis omkring hacking abgrebet.

**echo 1 > /proc/sys/net/ipv4/ip\_forward**

Denne kommando bruges til at broadcaste falske reply-messages

**arpspoof -i eth0 -t IP\_FOR\_YOUR\_LAPTOP -r IP\_FOR\_YOUR\_GATEWAY**

**Monitoring af ARP spoofing**

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse