Week-06 Network/network protocols and Security

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

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

Det er det laveste lag i TCP/IP suiten. Den bruges til at sende pakker mellem internet-lager interfacet og to forskellige hosts på samme lag.

* **Internet layer**:

Dette lag har ansvaret for at sende pakker til flere netværk. Internet Protocol er den principielle komponent i dette lag, hvilket definerer to adresse systemer til identificering af netværk hosts og lokaliserer dem på netværket.

* **Transport layer**:

Etablerer grundlæggende data kanaler som applikationen bruger til ‘task-specific’ data udveksling. Dette lag leverer end-to-end message transfer services (host-to-host forbindelse). Protokoller i dette lag indeholder fejlhåndtering, segmentering, flow kontrol og applikation adressering (portnumre).

* **Application layer**:
* **Explain the purpose of the DNS system and the DHCP protocol**

DNS systemet fungerer som en telefonbog. Man kender ikke nødvendigvis nummeret på en given person, men kan slå navnet op og få det. DNS minder meget derom, idet man ikke nødvendigvis kender IP-adressen til en server, men kender domæne navnet.

Der er mange DNS servere, og hvis et DNS ikke kender til ip adressen forbundet med domæne navnet, søger den efter den nærmeste DNS og spørg dertil om en relation. Dette fortsættes indtil der er en DNS server der kender til domænet, og alle DNS servere i kæden får nu gemt relationen.   
  
DHCP er protocollen der overser udstedelse af ip adresser til enheder der er forbundet til routeren. DHCP styrer også hvorvidt om en enhed får lov til at beholde sin ip adresse hen over tiden.

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

klienten sender et GET request til serveren, hvortil serveren svarer med et 200 OK.

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

ARP protokollen er den der fortæller routeren hvilken enhed en ip adresse er forbundet til.

arp kommandoen er til at ændre i ARP.

* **Explain Conceptually strategies a hacker can use to attack:**
* **The DNS system:**

Lokal DNS hijack - en hacker installere Trojan malware på en brugers computer, og ændre den lokale DNS indstillinger til at videresende brugeren til en forkert side.

Router DNS hijack - de fleste routere har default passwords og firmware sårbarheder. en hacker kan overtage en router og ændre på DNS indstillingerne, som påvirker alle brugere forbundet til routeren.

Man in the middle DNS attack - en hacker opfanger kommunikation mellem en bruger og en DNS server, og give brugeren en anden ip adresse end den brugeren har bedt om.

Rogue DNS server - en hacker kan hacke en DNS server, og ændre dens indstillinger. Derved alle der får en tilknytning fra den DNS server bliver sendt til en forkert side.

Cache Poisoning - Her afhænger man ikke på at overtage en DNS server, men i stedet sender en forfalsket forespørgsel, som så har en anden ip adresse end originalt tilknyttet til domænenavnet.

* **The DHCP protocol**

Der er en begrænset mængde af adresser i adresse poolen hos en server der bruger DHCP, så ved et denial of service angreb kan denne begrænsede mængde hurtigt blive mættet, således at der ikke kan tilkobles andre, da der ikke er ledige adresser til rådighed.

* **The TCP-protocol**

Strategien hedder TCP/IP hijacking og er et hack på user sessionen på et sikret netværk. Den mest almindelige metode at bruge for at hacke en session, er ved at bruge **IP-spoofing**, hvor en hacker bruger source-routed IP pakker til at indsætte kommandoer i en aktiv kommunikation mellem to noder og dermed fremstå som en af de autentificerede brugere.  
Et alternativ er at bruge cross site scripting, hvor hackeren benytter sig af et malicious JavaScript til at fange en brugers session ID.

* **The ARP-protocol**

Hackere kan angribe ARP som kører på dit netværk til at få det til at ligne at deres system er dit, eller en anden autoriseret enhed.

* **Provide at least one “practical” example using one of the strategies explained above**