Um die Netzwerkeinstellungen in Vmware Worksation zu ändern, muss als Admin gestartet werden.

1.3. Um die Nics zuzuweisen muss in der jeweiligen VM unter einstellungen die entsprechenden NICs gesetzt werden.

1.4.1 Ubuntu VM

Statische IP-Adress-Zuweisung

Um Ihren Server so zu konfigurieren, dass es er eine statische IP-Adresse verwendet, fügen Sie die Methode static zur Anweisung der »inet«-Adressenfamilie für die entsprechende Netzwerkschnittstelle in der Datei /etc/network/interfaces hinzu. Im unten stehenden Beispiel wird davon ausgegangen, dass Ihre als erste erkannte Ethernet-Schnittstelle eth0 genannt wurde. Ändern Sie die Werte address, netmask und gateway so ab, dass sie den Erfordernissen für Ihr Netzwerk entsprechen.

auto eth0

iface eth0 inet static

address 10.0.0.100

netmask 255.255.255.0

gateway 10.0.0.1

# Erstes Subnetz

subnet 192.168.2.0 netmask 255.255.255.0 {

range 192.168.2.10 192.168.2.40;

}

<https://wiki.ubuntuusers.de/ISC-DHCPD/>

Danach muss der server mit „service dhcp3-server restart“ neu gestartet werden.

1.4.2 Windows XP

Hat automatisch IP-Addresse erhalten, da DHCP schon eingeschalten war

1.4.3 Kali VM

Hat DHCP Lease von Router erhalten

2. Network Reconnaissance

2.1 Network Ping Sweep

Wireshark hört auf NIC eth1, da hier auf die Kali VM im selben Netz hängt.

Mögliche Antwort: Hier wird erkennt wieviele User in einem Netz sind. Es wird auch die MAC Adresse des entsprechenden Hosts geschickt

Ping Sweep schickt ARP Request an jede Host Addresse im angegebenen Netzwerk.

2.2. OS Detection

Hier muss nun ein erkannter Rechner im Befehl angegeben werden

Nmap -O -v 172.16.1.X (128)

Es werden alle offenen Ports (ob UDP oder TCP) angezeigt. Welches Betriebssystem auf dem Host läuft

2.3. Email Sniffing

Unter Kali wird das selbe angezeigt wie unter Ubuntu

3. Aktive Attacken

3.1. ARP Poisoning

Ettercap laut howTo von Moodle nachgearbeitet

Beim ARP Poisoning wird die MAC Addresse der Kali VM im ARP Eintrag ausgetauscht.

In ettercap wird nun der user mit passwort angezeigt

**Wireshark nochmal ansehen!**

3.2. DHCP Spoofing

Ubuntu DHCP server stoppen -> service dhcp3-server start #[or stop, or restart, ...]

Dabei soll herauskommen, das bei einem /renew nur eine andere IP erhalten wurde.

3.3. SSL Capturing

Wenn der User das Zertifikat vom Kali akzeptiert, läuft alles über die KaliVM und über Wireshark können die verschlüsselten Pakete angesehen werden, nachdem eine https seite aufgerufen wurde. Da Kali nun den private key kennt, kann dieser die Daten entschlüssen und eventuelle passwörter usw. herausfinden.