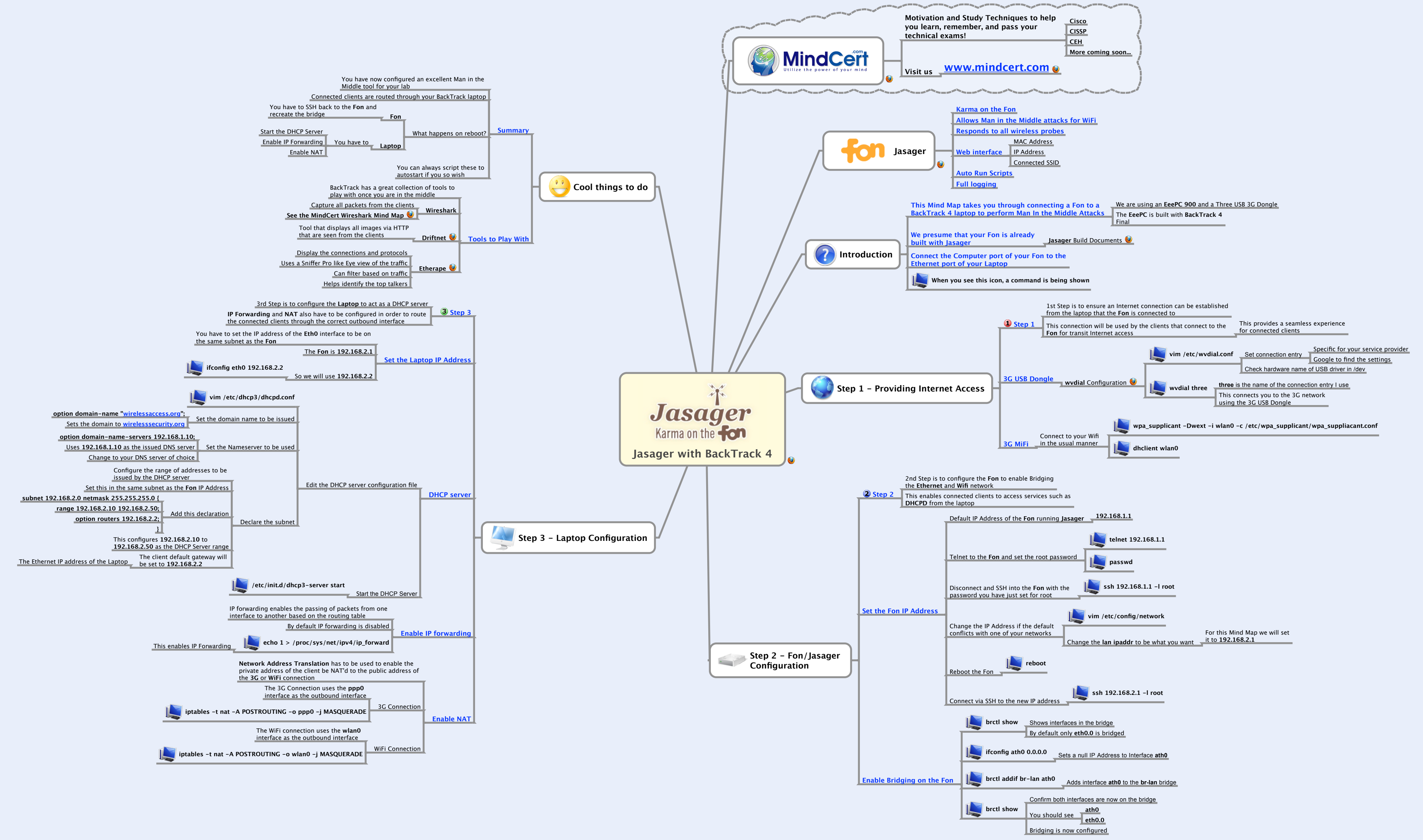

Jasager
Karma on the fon

Jasager with BackTrack 4

- MindCert.com — Utilize the power of your mind
  - Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
    - Cisco
    - CISSP
    - CEH
    - More coming soon...
  - Visit us
    - www.mindcert.com
- fon Jasager
  - Karma on the Fon
  - Allows Man in the Middle attacks for WiFi
  - Responds to all wireless probes
  - Web interface
    - MAC Address
    - IP Address
    - Connected SSID
  - Auto Run Scripts
  - Full logging
- Introduction
  - This Mind Map takes you through connecting a Fon to a BackTrack 4 laptop to perform Man In the Middle Attacks
    - We are using an **EeePC 900** and a Three USB 3G Dongle
    - The **EeePC** is built with **BackTrack 4** Final
  - We presume that your Fon is already built with Jasager
    - **Jasager** Build Documents
  - Connect the Computer port of your Fon to the Ethernet port of your Laptop
  - When you see this icon, a command is being shown
- Step 1 – Providing Internet Access
  - ① Step 1
    - 1st Step is to ensure an Internet connection can be established from the laptop that the **Fon** is connected to
    - This connection will be used by the clients that connect to the **Fon** for transit Internet access
      - This provides a seamless experience for connected clients
  - 3G USB Dongle
    - **wvdial** Configuration
      - vim /etc/wvdial.conf
        - Set connection entry
          - Specific for your service provider
          - Google to find the settings
        - Check hardware name of USB driver in /dev
      - wvdial three
        - **three** is the name of the connection entry I use
        - This connects you to the 3G network using the 3G USB Dongle
  - 3G MiFi
    - Connect to your Wifi in the usual manner
      - wpa_supplicant -Dwext -i wlan0 -c /etc/wpa_supplicant/wpa_suppliacant.conf
      - dhclient wlan0
- Step 2 – Fon/Jasager Configuration
  - ② Step 2
    - 2nd Step is to configure the **Fon** to enable Bridging the **Ethernet** and **Wifi** network
    - This enables connected clients to access services such as **DHCPD** from the laptop
  - Set the Fon IP Address
    - Default IP Address of the **Fon** running **Jasager**
      - 192.168.1.1
    - Telnet to the **Fon** and set the root password
      - telnet 192.168.1.1
      - passwd
    - Disconnect and SSH into the **Fon** with the password you have just set for root
      - ssh 192.168.1.1 -l root
    - Change the IP Address if the default conflicts with one of your networks
      - vim /etc/config/network
      - Change the **lan ipaddr** to be what you want
        - For this Mind Map we will set it to **192.168.2.1**
    - Reboot the Fon
      - reboot
    - Connect via SSH to the new IP address
      - ssh 192.168.2.1 -l root
  - Enable Bridging on the Fon
    - brctl show
      - Shows interfaces in the bridge
      - By default only **eth0.0** is bridged
    - ifconfig ath0 0.0.0.0
      - Sets a null IP Address to Interface **ath0**
    - brctl addif br-lan ath0
      - Adds interface **ath0** to the **br-lan** bridge
    - brctl show
      - Confirm both interfaces are now on the bridge
      - You should see
        - ath0
        - eth0.0
      - Bridging is now configured
- Step 3 – Laptop Configuration
  - ③ Step 3
    - 3rd Step is to configure the **Laptop** to act as a DHCP server
    - **IP Forwarding** and **NAT** also have to be configured in order to route the connected clients through the correct outbound interface
  - Set the Laptop IP Address
    - You have to set the IP address of the **Eth0** interface to be on the same subnet as the **Fon**
    - The **Fon** is **192.168.2.1**
    - So we will use **192.168.2.2**
      - ifconfig eth0 192.168.2.2
  - DHCP server
    - Edit the DHCP server configuration file
      - vim /etc/dhcp3/dhcpd.conf
      - Set the domain name to be issued
        - **option domain-name "wirelessaccess.org";**
        - Sets the domain to wirelesssecurity.org
      - Set the Nameserver to be used
        - **option domain-name-servers 192.168.1.10;**
        - Uses **192.168.1.10** as the issued DNS server
        - Change to your DNS server of choice
      - Declare the subnet
        - Configure the range of addresses to be issued by the DHCP server
        - Set this in the same subnet as the **Fon** IP Address
        - Add this declaration
          - **subnet 192.168.2.0 netmask 255.255.255.0 {**
          - **range 192.168.2.10 192.168.2.50;**
          - **option routers 192.168.2.2;**
          - }
        - This configures **192.168.2.10** to **192.168.2.50** as the DHCP Server range
        - The client default gateway will be set to **192.168.2.2**
          - The Ethernet IP address of the Laptop
    - Start the DHCP Server
      - /etc/init.d/dhcp3-server start
  - Enable IP forwarding
    - IP forwarding enables the passing of packets from one interface to another based on the routing table
    - By default IP forwarding is disabled
    - echo 1 > /proc/sys/net/ipv4/ip_forward
      - This enables IP Forwarding
  - Enable NAT
    - **Network Address Translation** has to be used to enable the private address of the client be NAT'd to the public address of the **3G** or **WiFi** connection
    - 3G Connection
      - The 3G Connection uses the **ppp0** interface as the outbound interface
      - iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
    - WiFi Connection
      - The WiFi connection uses the **wlan0** interface as the outbound interface
      - iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
- Cool things to do
  - Summary
    - You have now configured an excellent Man in the Middle tool for your lab
    - Connected clients are routed through your BackTrack laptop
    - What happens on reboot?
      - Fon
        - You have to SSH back to the **Fon** and recreate the bridge
      - Laptop
        - You have to
          - Start the DHCP Server
          - Enable IP Forwarding
          - Enable NAT
    - You can always script these to autostart if you so wish
  - Tools to Play With
    - BackTrack has a great collection of tools to play with once you are in the middle
    - Wireshark
      - Capture all packets from the clients
      - **See the MindCert Wireshark Mind Map**
    - Driftnet
      - Tool that displays all images via HTTP that are seen from the clients
    - Etherape
      - Display the connections and protocols
      - Uses a Sniffer Pro like Eye view of the traffic
      - Can filter based on traffic
      - Helps identify the top talkers

Jasager.mmap – 22/02/2010 – Andrew Mason