Mission 2 README

File locations & explanations:

All of the DNS files can be found in the /etc/bind/ directory. There are zone and key subdirectories inside that directory. All of the scripts to run attack and defense are in the home directory under the cs4404 user.

Running Infrastructure:

On the 10.4.9.2 VM

- sudo sysctl net.ipv4.ip_forward=1 // This enables ip forwarding on the router VM
- sudo route add default gw 10.4.9.2 // Set the default gateway for packets
- sudo route add 10.4.9.5 gw 10.4.9.2// Set path to DNS VM
- sudo route add 10.4.9.3 gw 10.4.9.2// Set path to client VM
- sudo tcpdump -i eth0 src 10.4.9.3 // See all incoming traffic from the client VM

On the 10.4.9.3 VM

- Set the /etc/resolv.conf file to look for the nameserver bombast.com at 10.4.9.5
- sudo route add default gw 10.4.9.2 // Set the default gateway for packets
- sudo route add 10.4.9.5 gw 10.4.9.2// Set path to DNS VM
- Run any dns client such as dig or nslookup on bombast.bombast.com or verizon.bombast.com

On the 10.4.9.5 VM

- sudo service bind9 restart // Restart bind9 service

Running Attack:

Run all of the same commands needed for the infrastructure

On the 10.4.9.2 VM

- Instead of tcpdump: sudo intercept.py // This will start the packet sniffer to intercept traffic to verizon

Defense:

Run all of the same commands for the infrastructure and attack, also sign the keys as described in the main paper.

On the 10.4.9.3 VM

- sudo dnssec.py <hostname>

On the 10.4.9.1 VM (Mock VPN)

- sudo sysctl net.ipv4.ip_forward=1 // This enables ip forwarding on the router VM
- sudo route add default gw 10.4.9.1 // Set the default gateway for packets
- sudo route add 10.4.9.5 gw 10.4.9.1// Set path to DNS VM
- sudo route add 10.4.9.3 gw 10.4.9.1// Set path to client VM
- sudo tcpdump -i eth0 src 10.4.9.3 // See all incoming traffic from the client VM