NETWORK SECURITY
(Assignment 4)

DNS INJECT

Usage:

dnsinject [-i interface] [-h hostname] expression

-i Capture packets from the network device <interface> (e.g., eth0). If not specified, mydump should automatically select a default interface to listen on

-h Read a list of IP address and hostname pairs specifying the hostnames to be hijacked. If '-h' is not specified, dnsinject should forge replies for all observed requests with the local machine's IP address as an answer.

<expression> is a BPF filter that specifies a subset of the traffic to be monitored. This option is useful for targeting a single or a set of particular Victims.

List of Libraries to be installed:

1. Install pip
2. Install scapy using pip
3. Python version supported: 2.7 or above
4. Commands: python dnsinject.py -i ens33

Steps

1. Check if the packet is UDP and destination port is 53.
2. If the hostfile name is given, then check if the qname in the question part of the packet matches with any of the hostname in the hostfile given. If it does, then change the rdata in the in the dns answer packet and send the injected packet.
3. If the hostfile is not given, then inject every packet with attacker's IP.

DNS DETECT

Usage:

dnsdetect [-i interface] [-r tracefile] expression

-i Capture packets from the network device <interface> (e.g., eth0). If not specified, mydump should automatically select a default interface to listen on

-h Read packets from <tracefile> (tcpdump format). Useful for detecting DNS poisoning attacks in existing network traces.

<expression> is a BPF filter that specifies a subset of the traffic to be monitored. This option is useful for targeting a single or a set of particular Victims.

Steps

1. Check if the packet is UDP and destination port is 53.
2. Maintain a list of dns responses containing dns packet id, answer count, hostname and list of IPs in rdata of answer part of DNS.
3. Check if the packet arrived has any answer of type A. If does not have any such answer, ignore the packet.

4. If the packet's id matches with one of the responses in the existing dns responses list, then further loop around the total number of answers the packet contains. If the dns answer type is A, then match if rdata matches with any of the existing list of rdata in the dns responses list. If it matches, then the reply is not forged. Else, it is forged, print the rdata stored in the dns responses list corresponding to that hostname and id and with rdata of the current packet.
5. If the id of the packet does not match with any of the existing ids in the dns responses list then add the packet details into dns responses list.

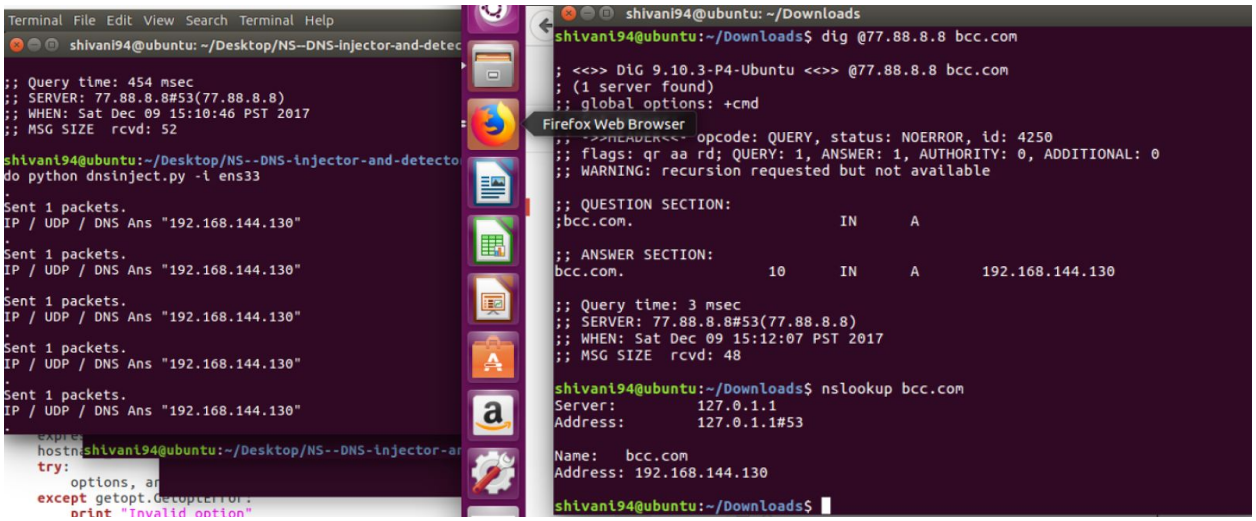
SAMPLE OUTPUTS

Run dig @77.88.8.8 bcc.com from one virtual machine

Run dns_inject command from another virtual machine and inject with attackers IP '192.168.144.130'

DNS detect output
DNS poisoning attempt
TXID 18513 Request bcc.com
Answer 1['184.168.221.96']
Answer 2['192.168.144.130']

DNS INJECT OUTPUT



DNS DETECT OUTPUT