(II) Poisoning DNS Cache (1)

(I)

- **Poisoning:** Attempt to put bogus records into DNS name server cache. [mapping b/w name for a host & its corresponding IP-address]
  - Bogus records could point to attacker nodes.
  - Attacker nodes could phish.

when clients queries & connects to that host name, it will be redirected to attackers machine

HARD

- But unsolicited replies are not accepted at a name server.
  - Name servers use IDs in DNS messages to match replies to queries.
  - So can't just insert a record into a name server by sending a DNS reply message.
- But can send a reply to a request.

(not like ARP poisoning map (MAC) IP)

(How to do it?)

(II)

Poisoning local DNS server (2)

Goal: Put bogus IP address for web.edu in local Berkeley DNS server.

1) Attacker queries local DNS server.
2) local DNS makes iterative queries.
3) Attacker waits for some time, sends a bogus reply spoofing authoritative server for web.edu

1) DNS query web.edu. local DNS server (eg Berkeley) may not have that mapping. (to resolve it, not have it in its cache)
2) ∴ it sends it to others (iterative DNS queries)
3) DNS reply web.edu = (17.32.8.9) (attacker machines IP)

(upper level servers)

(fake response as authoritative name server)

(III) Poisoned DNS server (eg Berkeley) has wrong mapping in its cache, some legitimate user queries, gets directed to attackers machine.
* DNS response can provide IP address of malicious server!

(IV) Issues:

- Attacker may need to stop upstream name server from responding.
  - so that server under attack does not get suspicious.
  - Ping of death, DoS, overflows etc.

done through.

Summary

- DNS is a critical component of the Internet infrastructure.
- But is surprisingly robust:
  - DDoS attacks against root servers have been largely unsuccessful (because of its distributed & hierarchial structure) ∴ robust
  - Poisoning and redirecting attacks are difficult unless you can sniff DNS requests
    - And even so, may need to stop DNS servers from replying.
- DNS can be leveraged for reflection against non-DNS nodes. (external machines).