Module 11
(dig, nslookup, zone transfer)

• At the end of this module, you should have an idea how the tools dig and nslookup can be used to find out about host names and IP addresses. You should know what a DNS zone is and how one might be able to identify all the information contained in a DNS zone file.
Dig and nslookup

- The old goto tool to identify the relationship between host names and IP addresses was nslookup.
  
  ```
  > nslookup cise.ufl.edu
  Server: 172.18.0.2
  Address: 172.18.0.2#53
  
  Non-authoritative answer:
  Name: cise.ufl.edu
  Address: 128.227.205.222
  ```

- nslookup has been obsoleted by dig:
  
  ```
  > dig cise.ufl.edu
  ...
  ;; QUESTION SECTION:
  ;cise.ufl.edu. IN A
  
  ;; ANSWER SECTION:
  cise.ufl.edu.19983 IN A 128.227.205.222
  ...
  ```
Reverse Lookups are Supported as Well

- Dig uses the -x parameter to denote reverse lookups:
  
  ```
  > dig -x 128.227.205.222
  ...
  ;;; QUESTION SECTION:
  ; 222.205.227.128.in-addr.arpa. IN PTR
  
  ;;; ANSWER SECTION:
  222.205.227.128.in-addr.arpa. 21600 IN PTR omaha.cise.ufl.edu.
  ```

- `nslookup` recognizes addresses as arguments:
  
  ```
  > nslookup 128.227.205.222
  ...
  Non-authoritative answer:
  222.205.227.128.in-addr.arpa name = omaha.cise.ufl.edu.
  ```
DNS Record Types

- A IPv4 address
- AAAA IPv6 address
- CNAME alias (mapping to another name)
- IPSECKEY Key record for Ipsec
- MX Mail exchange (list of mail transfer agents)
- NS Name server record
- PTR Pointer to a canonical name (for reverse lookup)
- SOA Start of Authority (identifies authoritative DNS zone)
- SRV Server specific records
DNS Zones

- A DNS zone is a portion of the DNS name space that has been delegated to an administrator who maintains a name server for that zone. Examples:
  - Edu
  - cise.ufl.edu
  - sploitlab.com
- The (often unfollowed) rule is that zone control should follow administrative control boundaries.
Zone Transfer

• Zone transfer used to be the stock in trade of nefarious internet evil-doers.

• nslookup used to support an `ls` command that would transfer all records maintained by a nameserver. That is now deprecated.

• `dig` still supports transfer of record type AXFR, but many servers refuse to honor it:

  ```
  > dig @ns.name.ufl.edu -t AXFR ufl.edu
  ; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @ns.name.ufl.edu -t AXFR ufl.edu
  ; (1 server found)
  ;; global options: +cmd
  ;; Transfer failed.
  ```

• Now OSINT and other techniques are used to try to tease this information out of public records and nameservers.
OSInt alternatives to Zone Transfer

• Kali includes a number of these.