JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Harvesting

THREAT MANAGEMENT

Why Use DNS?

- Often our first step in information gathering
- DNS information is publically available
- A quick Whois search can give you many details to use
- Hostnames can tell you about the server (DC1.jasondion.com might be a domain controller…)

nslookup

```
Command Prompt
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Benny>nslookup
Default Server:  cns3.tm.net.my
Address:  202.188.0.133

> www.cisco.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.cisco.com
Address:  198.133.219.25

> www.dlink.com
Server:  cns3.tm.net
Address:  202.188.0.133

Non-authoritative answer:
Name:    www.dlink.com
Address:  64.7.210.132

> exit

C:\Documents and Settings\Benny>
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

DNS Records

- MX (mail server records)
- A (address records)
- C (canonical records)
- PTR (pointer records)

tracert

```
Command Prompt

C:\>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list.
    -w timeout         Wait timeout milliseconds for each reply.

C:\>tracert 209.85.135.99

Tracing route to mu-in-f99.google.com [209.85.135.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    15 ms    14 ms    14 ms  172.29.64.217
  4    19 ms    19 ms    19 ms  gdr01-gdr11.ip.t-con.hr [195.29.240.74]
  5    32 ms    30 ms    31 ms  193.159.225.61
  6    38 ms    38 ms    37 ms  217.5.66.42
  7    41 ms    40 ms    41 ms  74.125.50.149
  8    42 ms    42 ms    43 ms  66.249.94.86
  9    42 ms    45 ms    41 ms  209.85.130.15
 10    43 ms    49 ms    54 ms  72.14.239.58
 11    42 ms    42 ms    43 ms  mu-in-f99.google.com [209.85.135.99]

Trace complete.

C:\>tracert www.google.com

Tracing route to www.l.google.com [209.85.135.99]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    15 ms    14 ms    14 ms  172.29.64.217
  4    20 ms    18 ms    18 ms  gdr01-gdr11.ip.t-con.hr [195.29.240.74]
  5    32 ms    31 ms    31 ms  193.159.225.61
  6    37 ms    76 ms   109 ms  217.5.66.42
  7    42 ms    41 ms    40 ms  72.14.198.117
  8    43 ms    46 ms    43 ms  66.249.94.86
  9    67 ms    41 ms    40 ms  209.85.130.21
 10    48 ms    53 ms    51 ms  209.85.253.22
 11    42 ms    43 ms    46 ms  mu-in-f99.google.com [209.85.135.99]

Trace complete.

C:\>
```

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE