

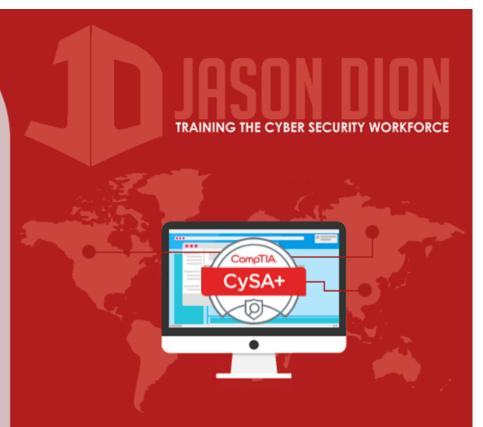


DNS Harvesting

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

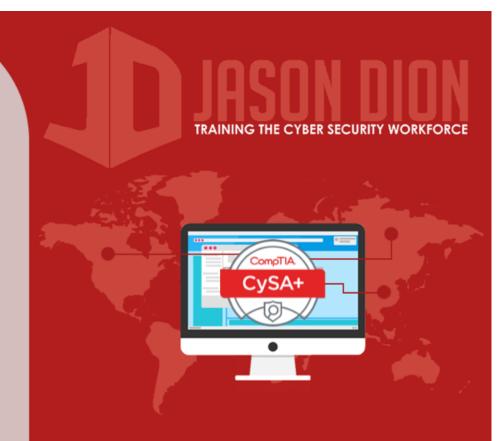
```
Command Prompt
(C) Copyright 1985-2001 Microsoft Corp.
C: Documents and Settings Benny inslookup
Default Server: cns3.tn.net.my
Address: 202.188.0.133
> www.cisco.com
Server: cns3.tm.net
Address: 202.188.0.133
Non-authoritative answer:
Name:
        www.cisco.com
Address: 198.133.219.25
> www.dlink.com
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>
```

TRAINING THE CYBER SECURITY WORKFORCE

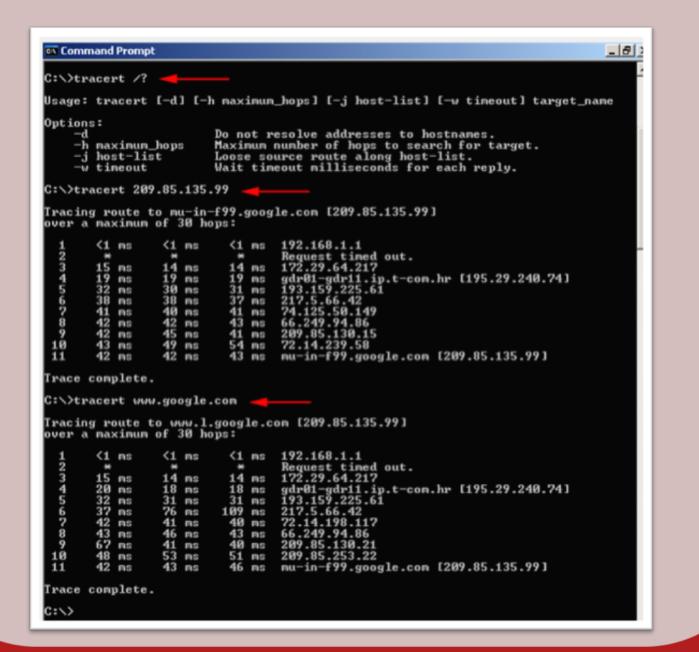


DNS Records

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



tracert



JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

