Becoming a Hacker

Passive Recon

John Allbritten
jallbrit@cisco.com
ASIG

Everett Stiles
evstiles@cisco.com
ASIG

Chris McCoy
cmm@cisco.com
ASIG

Omar Santos
osantos@cisco.com
PSIRT/Security Research & Operations

Sammy Tieng
stieng@cisco.com
ASIG

Passive == No Footprint on Target

- Generally a passive recon is going to find (mostly) public information about your target
- **No** attack network activity should be sent to the Target's network
- Maybe some e-mails, depends on your definition

Sources for Online Passive Recon

- Company's own website
- Other industry competitors
- Government websites
  - Regulatory
  - Registration
  - Courts
  - Trademark / Patent
- News / PR organizations
- Google
- LinkedIn
- Yahoo Answers
- StackExchange
- Whois / Registrars
- Twitter
- Facebook
- ….

Public Records Search

- Edgar - https://www.sec.gov/search-filings
- publicrecordsources.com
- lexisnexis.com
- intelius.com
- spokeo.com

Network Recon - RIRs

- Regional Internet Registrars (RIRs)

  whois [-h whois.<RIR>.net <ip address>

  - ARIN (US, Canada, parts of Caribbean, Antarctica)
  - RIPE (EU, Middle East, Central Asia)
  - APNIC (Asia, Australia, New Zealand, Pacific Islands)
  - AfriNIC (Africa, excluding middle east)
  - LACNIC (Central and South America, parts of Carribbean)

Whois cisco.com?

```
msf > whois cisco.com
[*] exec: whois cisco.com


Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: CISCO.COM
   Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
   Whois Server: whois.melbourneit.com
   Referral URL: http://www.melbourneit.com
   Name Server: NS1.CISCO.COM
   Name Server: NS2.CISCO.COM
   Status: clientTransferProhibited
   Updated Date: 03-apr-2012
   Creation Date: 14-may-1987
   Expiration Date: 15-may-2013

[….]

Domain Name.......... cisco.com
  Creation Date........ 1987-05-14
  Registration Date.... 2011-04-06
  Expiry Date.......... 2013-05-16
  Organisation Name.... Cisco Technology, Inc.
  Organisation Address. 170 W. Tasman Drive
  Organisation Address.
  Organisation Address.
  Organisation Address. San Jose
  Organisation Address. 95134
  Organisation Address. CA
  Organisation Address. UNITED STATES

Admin Name........... Info Sec
  Admin Address........ 170 West Tasman Drive
  Admin Address........
  Admin Address........
  Admin Address. San Jose
  Admin Address........ 95134
  Admin Address........ CA
  Admin Address........ UNITED STATES
  Admin Email.......... infosec@cisco.com
  Admin Phone.......... +1.4085273842
  Admin Fax............ +1.4085264575

Tech Name............ Network Services
  Tech Address......... 170 W. Tasman Drive
  Tech Address.........
  Tech Address.........
  Tech Address......... San Jose
  Tech Address......... 95134
  Tech Address......... CA
  Tech Address......... UNITED STATES
  Tech Email........... dns-info@cisco.com
  Tech Phone........... +1.4085279223
  Tech Fax............. +1.4085267373
  Name Server.......... NS1.CISCO.COM
  Name Server.......... NS2.CISCO.COM
```

Network Recon -- ARs

- Accredited Registrars (ARs)
  - Top level domain registrars
    - gTLD – Global - .com, .net
    - ccTLD – Country code - .us, .ca, .eu. .de, .au, etc..
  - ICANN regulated
  - Use first level domain for gTLDs: whois fubar.com
  - First or second level for ccTLDs: whois [fubar.us | fubar.co.uk]

Network Recon – IP Netblocks

- Whois also finds ownership of Netblocks
  whois 192.168.1.1
- Not always 100% but good enough for gov't work
- All public information and lots of on-line tools to help, some at a fee so beware!
- IP2GeoLocation Lookup Databases
  - https://www.maxmind.com/en/geolocation_landing
  - https://www.ultratools.com/tools/geoIp
  - http://freegeoip.net/static/index.html

Whois 171.68.46.188 (ssh-sjc-2.cisco.com)

```
msf > whois 171.68.46.188
[*] exec: whois 171.68.46.188

#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 171.68.46.188"
#
# Use "?" to get help.
#
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=171.68.46.188?showDetails=true&showARIN=false&ext=netref2
#

Cisco Systems, Inc. NETBLK-CISCO-BBLOCK (NET-171-68-0-0-2) 171.68.0.0 - 171.69.255.255
BBN Communications NETBLK-BARRNET-BBLOCK (NET-171-68-0-0-1) 171.68.0.0 - 171.71.255.255
Asia Pacific Network Information Centre APNIC-ERX-171 (NET-171-0-0-0-0) 171.0.0.0 - 171.255.255.255
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
```

Domain Name Services

- DNS holds lots of information, most really nice to know
  - Multiple enumeration tools available: nslookup, dig, host
    - Ex: dig –t any cisco.com
  - Scripts all over the place!
    - Metasploit: auxiliary/scanner/gather/enum_dns
  - Illegal in some jurisdictions :-p
- WINS – Windows Internet Name Service is similar for NetBIOS Name Services
  - Multiple GUI tools -- ‘net’ is used in Windows CLI & Samba
- Umbrella Investigate

Using Metasploit to Enumerate DNS

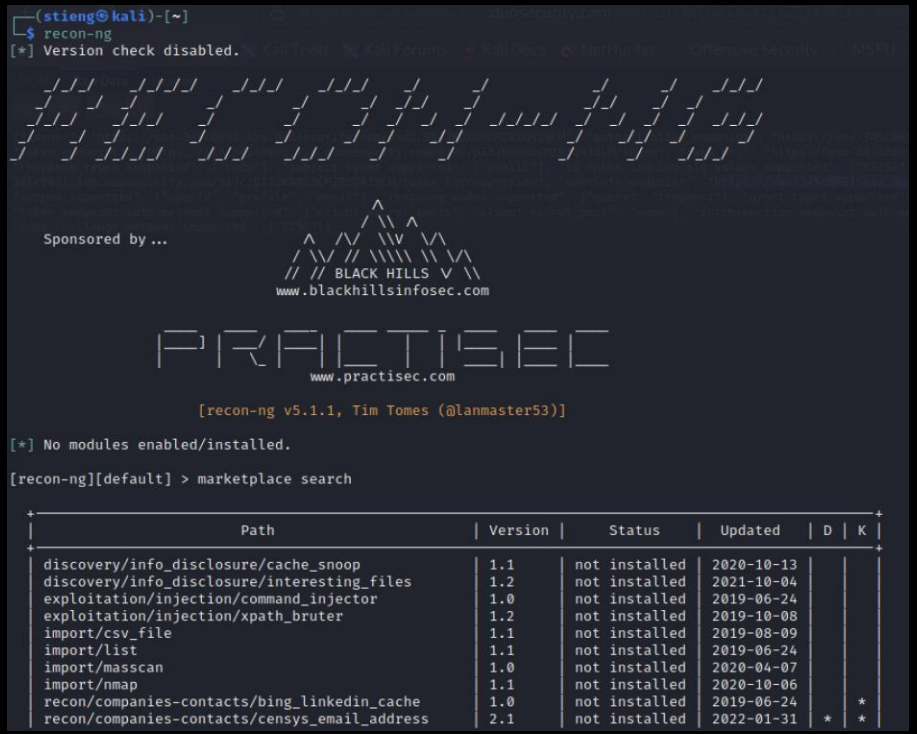
```
msf > use auxiliary/gather/enum_dns
msf  auxiliary(enum_dns) > show options

Module options (auxiliary/gather/enum_dns):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   DOMAIN                                                        yes       The target domain name
   ENUM_AXFR    true                                             yes       Initiate a zone transfer against each NS record
   ENUM_BRT     false                                            yes       Brute force subdomains and hostnames via the
supplied wordlist
   ENUM_IP6     false                                            yes       Brute force hosts with IPv6 AAAA records
   ENUM_RVL     false                                            yes       Reverse lookup a range of IP addresses
   ENUM_SRV     true                                             yes       Enumerate the most common SRV records
   ENUM_STD     true                                             yes       Enumerate standard record types (A,MX,NS,TXT and
SOA)
   ENUM_TLD     false                                            yes       Perform a TLD expansion by replacing the TLD with
the IANA TLD list
   IPRANGE                                                       no        The target address range or CIDR identifier
   NS                                                            no        Specify the nameserver to use for queries (default
is system DNS)
   STOP_WLDCRD  false                                            yes       Stops bruteforce enumeration if wildcard
resolution is detected
   WORDLIST     /opt/metasploit/msf3/data/wordlists/namelist.txt  no        Wordlist for domain name bruteforcing
msf auxiliary(enum_dns) > set DOMAIN target.com
msf auxiliary(enum_dns) > set ENUM_AXFR false
msf auxiliary(enum_dns) > set ENUM_BRT true
msf auxiliary(enum_dns) > run
```

Recon-ng

- OSINT framework similar to Metasploit exploitation framework
- Consists of a series of modules run in their own workspace
- Perform wide range of reconnaissance activities on different settings



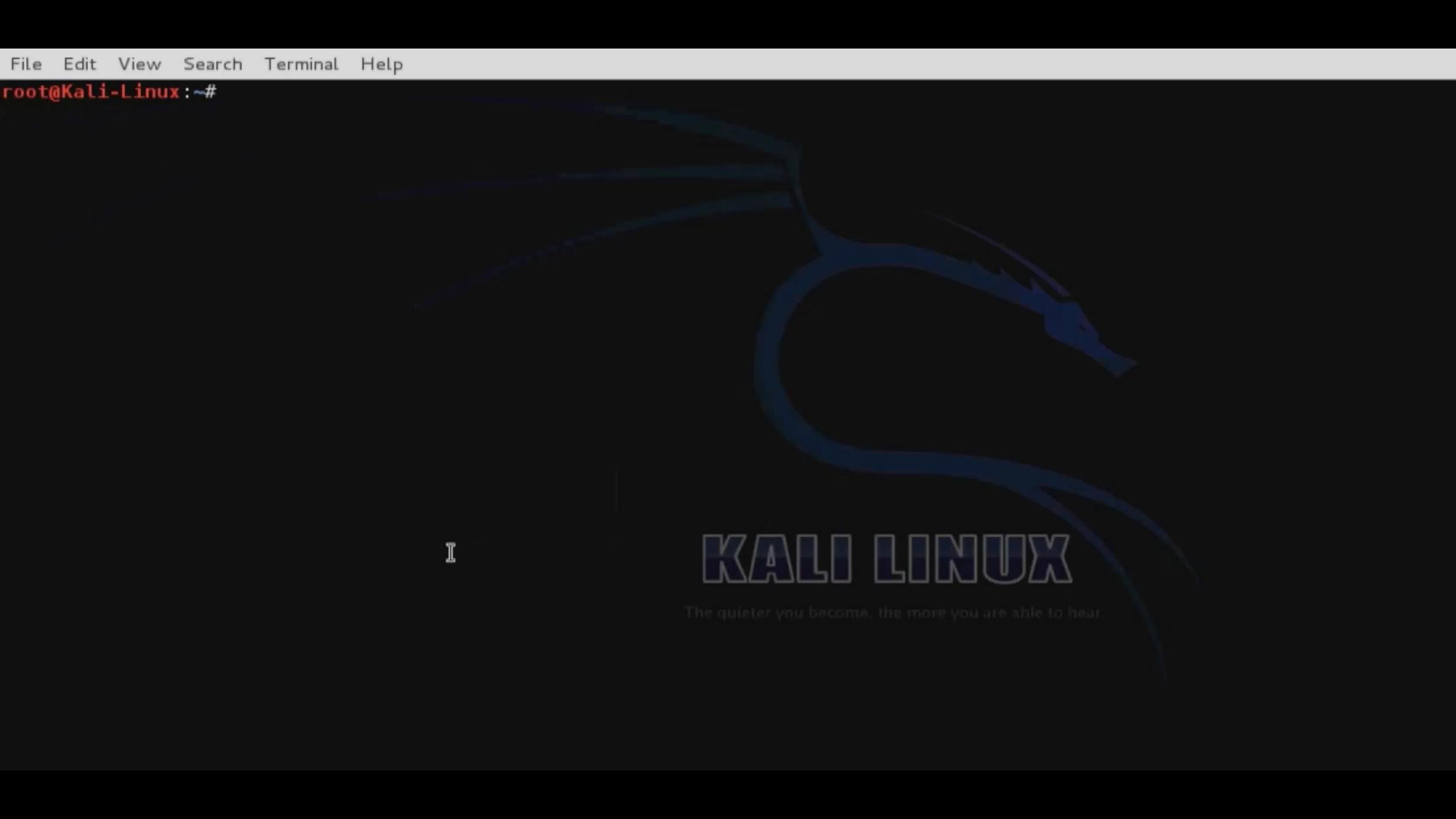
theHarvester

- Recon/OSINT toolkit
- Gathers names, emails, IPs, subdomains, etc.
- A collection of modules
  - Mostly 3rd party

Dmitry demo

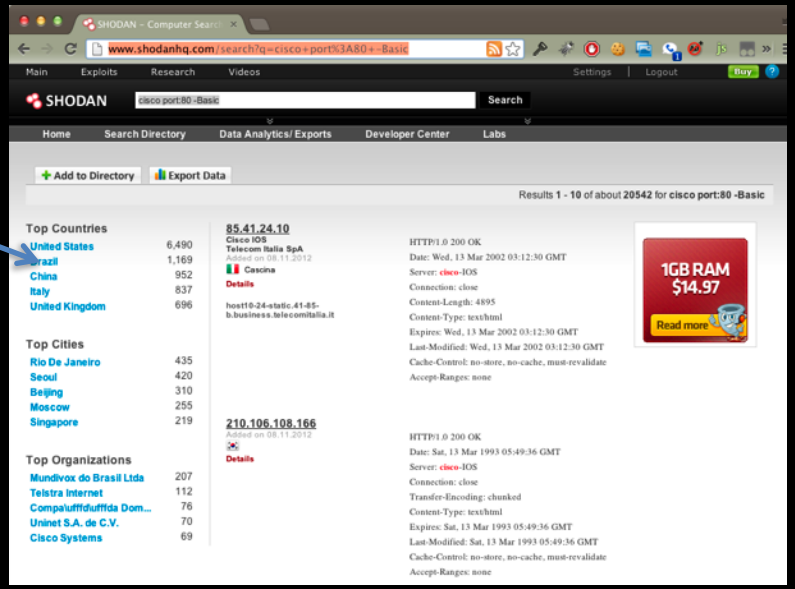
File Edit View Search Terminal Help

root@Kali-Linux:~#



Shodan – Internet Scanner

- https://www.shodan.io
- HTTP, SSH, Telnet, SNMP
- cisco port:80 -Basic



cisco

SecCon **2014**

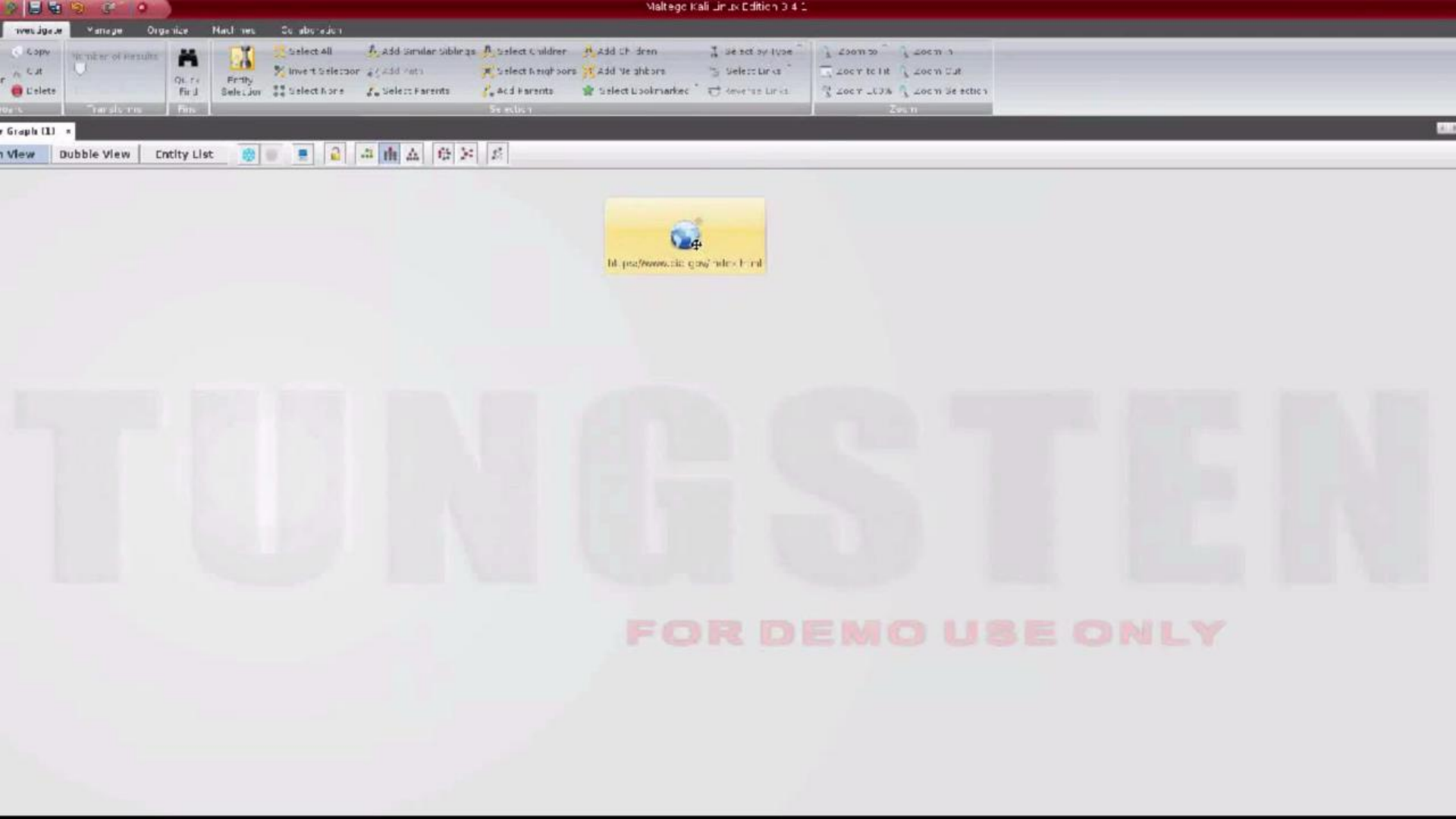
Securing the Internet of Everything

shodanhq.com

SHODAN

Maltego

- Paterva's Maltego helps to collect and correlate multiple information into a useable interface.
- http://maltego.com
- Many "Transforms" that will take data, like a subnet or domain name, and turn it into actionable data
- Helps to identify relationships


Select All
Invert Selection
Select More
Select Parents
Select Children
Select Neighbors
Add Parents
Select Bookmarked
Zoom In
Zoom Out
Zoom to Fit
Zoom Selection
Graph (1)
View
Bubble View
Entity List
TUNGSTEN
FOR DEMO USE ONLY

E-Mail Headers

- E-Mail headers provide a fair amount of information about a target company.
  - Find e-mail addresses on the Internet
  - Send random inquiries that need responses
  - Review the headers!
- Some cool headers:
  - X-Originating-IP: <target's workstation IP>
  - User-Agent: Target's E-Mail Client and Version
  - X-Mailer: Another place where E-Mail Client and Version may be
  - Received: The path the of the SMTP chain

Lab Exercise

becomingahacker.com