Information Gathering Techniques

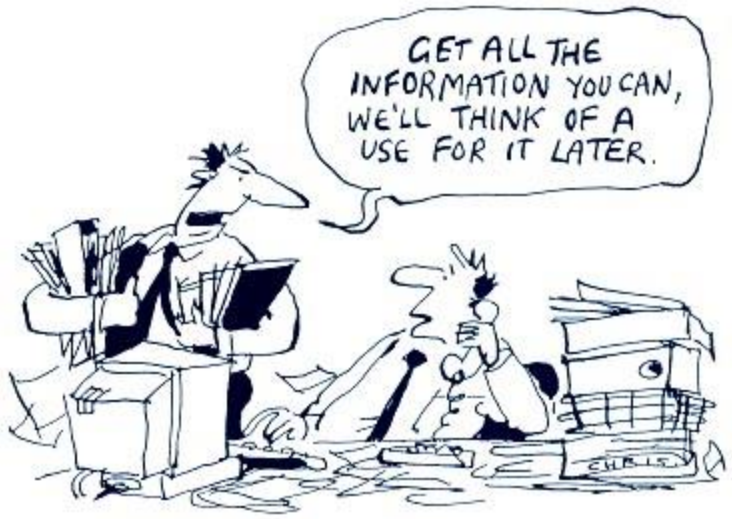
February 20, 2013

Ethical Disclaimer

- This is for testing and educational purposes only. Do not use any of the methods described and or discussed for illegal purposes.
- Only methods for gathering public information can be attempted outside of a test environment.
- Any intrusive activities such as port scanning or service probing should be done in test environments only.

Introduction

- Bit9 hacked in order to attack companies using their application white listing product.
  - https://securosis.com/blog/karma-is-a-bit9h



PTES Intelligence Gathering

- Reconnaissance against a target to gather as much information as possible.
- The more information gathered increases the chances of identifying potential attack vectors.
- www.pentest-standard.org

Types of Intelligence Gatering

- Open Source Intelligence (OSINT)
  - Produced from publicly available information
- Footprinting
  - Phase of info gathering that identifies the technical profile or surface area
- Human Intelligence (HUMINT)
  - Involves interactions whether physical or verbal

Gathering DNS Intelligence

- DNS – Service used for translating hostnames to IP addresses
- Why do we care?
  - Publicly available information:
  - Registrar Information
  - Mail Information
  - IP Addresses
  - Servers
  - Devices
  - Services and Applications

DNS Techniques

- Record Types:
  - A, AAAA, CNAME, PTR, MX, NS
- Whois
- Forward/Reverse DNS
  - Nslookup, host, dig
- DNS Bruteforce

DNS Tools

- DNSenum, DNSmap, etc
  - A records
  - MX records
  - Brute force options with provided dictionary
  - Check for zone transfer
  - Beware of wildcard entries

General BackTrack Usage

```
root@bt:/pentest/enumeration/dns# cd dnsenum/
root@bt:/pentest/enumeration/dns/dnsenum# pwd
/pentest/enumeration/dns/dnsenum
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl
dnsenum.pl VERSION:1.2.2
Usage: dnsenum.pl [Options] <domain>
[Options]:
Note: the brute force -f switch is obligatory.
GENERAL OPTIONS:
  --dnsserver   <server>
                        Use this DNS server for A, NS and MX queries.
  --enum                Shortcut option equivalent to --threads 5 -s 20 -w.
  -h, --help            Print this help message.
  --noreverse           Skip the reverse lookup operations.
  --private             Show and save private ips at the end of the file domain_ips.txt.
  --subfile <file>      Write all valid subdomains to this file.
  -t, --timeout <value> The tcp and udp timeout values in seconds (default: 10s).
  --threads <value>     The number of threads that will perform different queries.
  -v, --verbose         Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
  -p, --pages <value>   The number of google search pages to process when scraping names,
                        the default is 20 pages, the -s switch must be specified.
  -s, --scrap <value>   The maximum number of subdomains that will be scraped from Google.
BRUTE FORCE OPTIONS:
  -f, --file <file>     Read subdomains from this file to perform brute force.
  -u, --update  <a|g|r|z>
                        Update the file specified with the -f switch with valid subdomains.
        a (all)         Update using all results.
        g               Update using only google scraping results.
        r               Update using only reverse lookup results.
        z               Update using only zonetransfer results.
  -r, --recursion       Recursion on subdomains, brute force all discovred subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
  -d, --delay <value>   The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
  -w, --whois           Perform the whois queries on c class network ranges.
                         **Warning**: this can generate very large netranges and it will take lot of time to performe reverse lookups.
REVERSE LOOKUP OPTIONS:
  -e, --exclude <regexp>
                        Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
  -o --output <file>    Output in XML format. Can be imported in MagicTree (www.gremwell.com)
root@bt:/pentest/enumeration/dns/dnsenum#
```

Google Hacking

- Technique using Google Search to find information, configurations, files, and any other information indexed by Google.
- Why do we care?
  - Purposefully or accidently shared information is easily found
  - Files, configurations, default installations, and other specific files are valuable targets
  - Target attack versus opportunistic

Google Search Operators

- Uses special search operators in Google to find specific results:
  - Olympics site:.gov
  - Proftpd Filetype:conf
  - Inurl:proftpd.conf
  - http://support.google.com/websearch/bin/answer.py?hl=en&answer=136861

Google Hacking

- Google Dorks
  - http://www.exploit-db.com/google-dorks/
- Google Hacking DB
  - http://www.hackersforcharity.org/ghdb/

Google Hacking Tools

- Metagoo
  - Found in BackTrack
  - PDFs, word documents, excel spread sheets, etc.
- Goohost
  - Found in BackTrack
  - Gather DNS records with IP address using Google

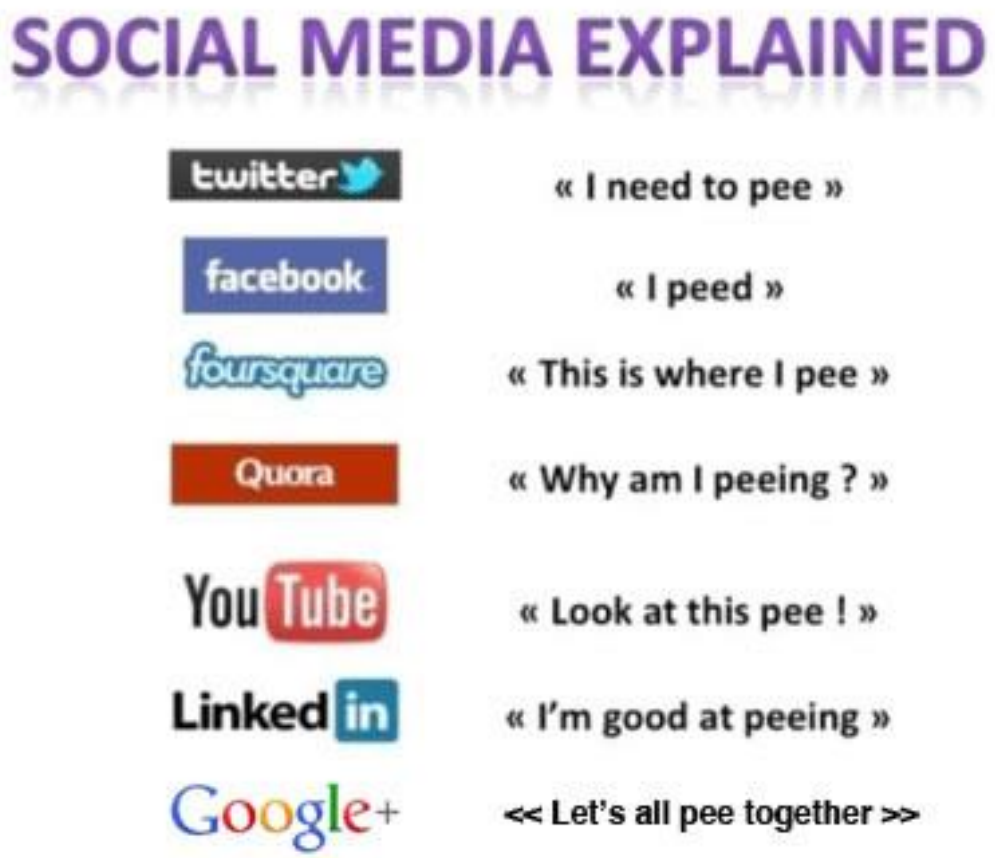
Email Gathering

- List of emails can be useful
  - Possible login names
  - Phishing Targets
  - Additional information searching with email
- theHarvester.py
  - Found in BackTrack
  - ./theHarvester.py -d <<target domain>> -b google -l 500

Social Networks

- Open forum for sharing personal and company information
- Why do we care?
  - Answers to security questions can be found
  - Organizational structure
  - Relaxed perception of private and public sharing
  - Geographic location and real-time status

This Says it All



SecMN

Social Networking Tools

- Maltego
  - Found in BackTrack
- Additional tools to consider:
  - Pushpin.py
  - Cree.py
- Manually searching social media

Putting it all Together

- Analyzing technical info gathered to create a network diagram
  - Valuable in understanding surface area
  - Technical structure and services
- Analyzing employee info gathered to create an Org Chart
  - Valuable in social engineering attacks.
  - Name dropping key people
  - Understanding business processes and functions

Hands On

- Challenges
  - Using any of the tools and methods discussed:
    - Gather detailed DNS information for a domain of your choice
    - Harvest contact information for a company of your choice
    - Utilize metaGoo for a domain of your choice
  - Be the first to submit results for any of the items above to pick a prize.