Open Source Intelligence Gathering

Non-intrusive methods of fingerprinting a target.

Kyle Osborn (@theKos)

AppSec Consulting (@AppSecConsult)

Who Am I?

- Kyle Osborn (.com)
  - @TheKos
  - Information Security Specialist (PenTester)
- Past Presentations
  - ChromeOS browser extension security
    - BlackHat USA, DefCon, BSidesLV
  - XSS Inside Desktop/Mobile Application
    - Toorcon Seattle/SanDiego, DerbyCon, TakeDownCon

Who Are We?

- AppSec Consulting
  - WebApp, Network & Physical security testing
  - Code Review
  - PCI Compliance
  - Training
  - Ninjas

What is a PenTest?

- Actually a multi-step process
  1) Intelligence [**Information**] Gathering
     - Intrusive
     - Non-intrusive
  2) Analyzing
     - Draw conclusions to possible attack vectors & scope
  3) Attack
     - Use what we derived from 1 & 2 to exploit our target.
  4) Rinse and repeat (as required)

So what is ”Intelligence” gathering?

- Used at the beginning of an attack
- Define scope
- Discover attack vectors

- **O**pen **S**ource **Int**elligence (OSINT) is

Jump right into it:

- DNS records
- Domain information
- Search Engines
- Social Media

DNS Records

- A, AAAA, MX, TXT records
- Lots of data
- Sometimes internal

- Discover subdomains

Zone Transfers

- Wealth of data

dig @ns1.secure.net owasp.org axfr

```
owasp.org.      86400IN  A   216.48.3.18
*.owasp.org.        86400IN  CNAME   owasp.org.
ads.owasp.org.      86400IN  A   216.48.3.26
austin.owasp.org. 86400IN  CNAME   owasp.org.
docs.owasp.org.         86400IN  CNAME   ghs.GOOGLE.COM.
es.owasp.org.       86400IN  A   216.48.3.18
```

DNS Records

- A, AAAA, MX, TXT records
- Lots of data
- Sometimes internal

- Discover subdomains

DNS Records

- Bruteforcing
  - Can lead to hidden subdomains
  - But can be noticed
- Fierce V2
- DNSMap

Reverse DNS (ptrs)

- From IP → Hostname

  nslookup 216.12.146.148

  Non-authoritative answer:

  148.146.12.216.in-addr.arpa name = www.isc2.org.

- New tool released by Rob Fuller (@Mubix)
- https://www.deepmagic.com/

Reverse DNS (ptrs)

https://www.deepmagic.com/ptrs/ptrs?search=isc2.org

64.224.81.109 list.isc2.org

68.238.174.237 wug.isc2.org

149.20.80.51 isc2.ext2.inet.tech.org

149.20.80.43 isc2.ext1.inet.tech.org

WHOIS data

- Works on IP & Domains

- Whois google.com
- Whois 4.2.2.2

Search Engines

- ”Google Dorking”
  - Site: inurl:
- Bing searches
  - Ip:

Tools

- Lots of tools.
- Lots can be done by hand.
-
- http://securitytube-tools.net/index.php?title=Information_Gathering

Thanks

- Talk to me after.
- Follow me on Twitter. @theKos
- Email me. kosborn@appsecconsulting.com