eJPT Certification

Section: Penetration Testing

08/7/2020

**Learning Objectives:**

* What is OSINT?
* Basic techniques of collecting information about your target.

**Information Gathering**

* Helps us understand the target organization, widen the attack surface and mount efficient and targeted attacks.

**Open-Source Intelligence**

* Why is it important?
  + Widens the attack surface.
  + Mounting targeted attacks.
  + Sharpening your tools in preparation for the next phases.
* Getting open source intel a few years ago used to look like the following:
  + Getting info from the press.
  + Looking up addresses and phone numbers in phone directories.
  + Visiting he company web site to get information about systems and products.
  + Now… we can accomplish the same thing by leveraging social networks, public sites, and visiting the company websites.
* **Social Networks Information Gathering**
  + The weakest link in the security chain is humans.
  + When employees of a company post information on social media about current projects, trips to conferences, phone numbers, and email addresses they are enabling criminals to build sophisticated profiles, which can be used to conduct phishing and impersonation attacks.
  + Choosing which social network to probe for intelligence gathering depends on the target client and the type of engagement.
    - For example: if the client is an advertising company, checking Instagram would be a great choice.
  + For LinkedIn specific examples reference slides.
  + Public Sites Information Gathering- reference slides starting at 1.2.2.
  + To find companies who have worked with the USA government we can check resources like [SAM](https://www.sam.gov/SAM/) (System for Award Management) and the [GSA eLibrary](https://www.gsaelibrary.gsa.gov/ElibMain/home.do)
    - Provides information about contracts between private companies and the US Gov’t.
* Whois
  + Whois is a database that contains information such as:
    - Owner name
    - Street addresses
    - Email addresses
    - Technical contacts.
    - Etc.
  + Regarding an internet domain name.

**Subdomain Enumeration**

* Many companies also share the same top-level domain name. Ex: careers.company.com, mail.company.com, or business.company.com
  + Subdomain enumeration can identify additional resources of target.
  + This increases the attack surface.
* Some cases show that subdomain sites from even larger companies can become neglected containing buggy software, sensitive information, or even administrative interfaces that are not secured.
* Passive Subdomain Enumeration- trying to ID subdomains without directly interacting with the target, but through open sources.
  + Passive Subdomain Enumeration tool: dnsdumpster.com
    - Uses data from google-indexed subdomains, but also checks sites like Bing or virustotal for similar information.
  + Another tool: sublist3r- extends DNS enumeration- [github repo](https://github.com/aboul3la/Sublist3r)
    - Collects DNS data from various sources.
    - NOTE: This tool can easily be blocked by Google (Google search engine does not like automated tools).
    - To run a basic command in bash the -d[domain] flag, and it will start searching for subdomains from various sources.
      * *Command- sublist3r -d example.com*

**The Importance of Information Gathering**

* Good penetration testers spend 90% of his time widening the attacks surface because he knows this is what it’s all about.
* The other 10% is done launching the correct commands with the appropriate tool with a high success rate.
* Penetration testing is a cyclic process. Each time you get deeper inside a client’s infrastructure you gain more information.