**Module 2 Footprinting**

**2.1 Footprinting**

**Footprinting**

1. Footprinting – technique for gathering info on comp systems & entities they belong to

**Active & Passive**

1. Active – interaction
   1. Eg. Meeting in person, port scanning, sharing coffee
2. Passive – publicy available

**Benefits of Footprinting**

1. Know security posture
   1. What OS, servers etc using
2. Reduce focus area
   1. Eg. If running windows no need do linux stuffs
3. Identify vulnerabilities
4. Network map

**How to Footprint**

1. Search engines
2. Google hacking
   1. Use strings to try to find password files
   2. Special search strings to find information
3. Shodan
   1. See vulnerable devices they have on internet
   2. Search engine for IoT devices (AKA Hacker’s search engine)
4. Whois
   1. See info on domain name
5. Social media
6. Competitive intelligence
7. Job boards
   1. Find general targets by fishing targets by listing jobs
8. Alerts
   1. Get alerts from websites
   2. <https://visualping.io/>
9. Mirror website
   1. <https://www.httrack.com/>
   2. Find info and find vulnerabilities
10. Email footprinting
    1. The harvester – tool in linux

**Tools**

1. Maltego
   1. Maps out website/servers
2. Recon-ng
3. OSRFramework

**Google Hacking**

1. Google Hacking – allows us to use specific strings to narrow down search results & potentially locate usernames, passwords etc.
   1. AKA Google Dorking
   2. However, google frequently disables some of these so Google Hacking Database site is going to be great long-term resource of what still works
2. Google hacking database
   1. <https://www.exploit-db.com/google-hacking-database>
3. Eg. “password.xlsx” ext:xlsx
   1. Fish out password files of random websites
   2. However if you keep using these commands google might think you a bot so must do stuff that verifies you’re a human
4. filetype : type – searches specific file types
   1. Eg. Filetype: doc – only search word docs
5. Intitle: string – search pages containing string intitle
6. Inurl: string – displays pages with string in URL
7. site: domain – displays pages for specific website/domain
   1. Eg. site:Microsoft.com passwds – show all pages with text passwds in website

**NIKTO**

1. Nikto tool – gather info form website
   1. Specifically look for possible vulnerabilities on website
2. nikto –e 1 –h webscantest.com
   1. –e use evasion switch & number 1 (to specify random encoding) to help us be a bit stealthier when running scan
   2. Use –h to define hostname/IP address
3. In this case, the website has these vulnerabilities
   1. Anti-clickjacking header not present
   2. XSS protection header not defined
   3. Etc.

**TheHarvester**

1. theHarvester – useful for gathering info on subdomains, employee names, emails, open ports & banners
   1. gathers info from public sources (Eg. search engines & shodan)
2. theHarvester –d Microsoft.com –l 50 –b google –h myresults.html
   1. –d is domain/company name to search
   2. –l is to limit the results (50 results)
   3. –b to define data source (google)
   4. –h allow us to use Shodan database to query any discovered hosts

**Shodan**

1. Shodan – hacker’s search engine
2. Go to <https://www.shodan.io/>
   1. Register account
   2. Can search for devices & filter countries etc