Footprinting and Reconnaissance

Hyperlinks for each chapter

Chapter 0 Introduction

00_01 Scouting the target

- For a summary of the objectives for the Certified Ethical Hacker (CEH) visit: https://cert.eccouncil.org/announcements.html

00_02 Comparing network attacks

- No links

00_03 Hacking Ethically

- No links

Chapter 1 Footprinting and Reconnaissance Low Tech

01_01 Footprinting and Reconnaissance

- No links

01_02 Using Competitive Intelligence

- Here we see a list of PeopleSoft vulnerabilities: https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-6013/Oracle-Peoplesoft-Enterprise.html

01_03 Using Google hacking to find information

- To find out how search engines locate information visit: https://research.google/pubs/pub37043/
- To do an advanced search in Google visit: https://www.google.com/advanced_search
- Here you'll find the Google hacking database: https://www.exploit-db.com/google-hacking-database

01_04 Searching with advanced operators

- No links

01_05 Getting Social

- No links

01_06 Using AnyWho - Spokeo - Yansi

- To find information on a person visit https://www.anywho.com/
- Spokeo is an advanced people search. To use visit: https://www.spokeo.com/
- Visit Zabasearch to find out information on someone: https://www.zabasearch.com/
- For advanced searches using PiPl visit: https://pipl.com/
- To get help during genealogy research visit: http://www.censusfinder.com/
- To search United States Birth Certificates, Death Records & Marriage Licenses visit: https://vitalrec.com/

01_07 Tracking Online Reputation

- To make sense of a ton of information, use https://webhose.io/
- To create a spider and search a URL to drill down on your target, visit: https://portia.readthedocs.io/en/latest/getting-started.html
- Improve the efficiency of your website by using tools found on: https://www.tapclicks.com/platform/sem-seo/
- Search for images using Google by going to: https://www.google.com/imghp
- Google alerts can be found here: https://www.google.com/alerts

Chapter 2 Using Email and Websites

02_01 Footprinting websites and email (Title change)

- To generate a list of possible email addresses visit: https://getmara.com/static/email-address-generator.html

02_02 Mirroring websites

- To copy a website visit: https://www.httrack.com/

02_03 Challenge: Mirror a website

- To copy a website visit: https://www.httrack.com/

02_04 Response: Mirror a website

- Here is the site example.com: http://example.com/
- To see the actual Center for Disease and prevention visit: https://www.cdc.gov/
- Learn how to spot a cloned website https://www.infinityinc.us/attack-of-the-clones-how-to-avoid-the-website-cloning-trap/
- Learn how to spot a phishing attack: https://www.infinityinc.us/how-to-spot-phishing-attack/

02_05 Monitoring websites

- Google analytics can help you make sense of your web traffic: https://marketingplatform.google.com/about/analytics/
- Visit https://www.pingdom.com/website-monitoring to gather website analytics
- To monitor the uptime of your website visit: https://updown.io/
- To get the scripts to monitor your Website and APIs from your computer go to GitHub: https://github.com/sanathp/statusok
- Using this site will help you do a quick check to see if a site is up and responding: https://montastic.com/
- For help with website traffic analysis go to: https://www.similarweb.com/
- To gain insight on your audience visit: https://www.quantcast.com/products/measure-audience-insights/

02_06 Investigating email

- No links

02_07 Using OSINT Tools

- To learn more about Maltego and download the community edition visit: https://www.maltego.com/

02_08 Challenge: understanding email headers

- Use the exercise file: 02_08 Challenge Email Header
- Visit mxtoolbox to investigate an email header: https://mxtoolbox.com/public/content/emailheaders/

02_09 Response: understanding email headers

- Visit mxtoolbox to investigate an email header: https://mxtoolbox.com/public/content/emailheaders/

Chapter 3. Discovering Reconnaissance tools

03_01 Footprinting using DNS

- To grab a packet capture on DNs go to Chris Sanders https://github.com/chrissanders/packets

03_02 Generating Domain Names

- To download a copy of Domain Name Analyzer, go to: https://domainpunch.com/dna/download.php

03_03 Using Subdomains

- No links

03_04 Understanding ICMP

- No links

03_05 Using PING and tracert

- No links
- ***NOTE**: PathPing is only available on Windows, if you are using Kali Linux you can install mtr, which provides similar functionality. Type: sudo apt install mtr*

03_06 Analyzing the Path

- To see a non-graphical trace, ping and other tools online go to: Networktools.com
- To do a visual path analysis visit https://www.pathanalyzer.com/
- VisualRoute helps with troubleshooting as it shows you the path taken from point A to point B: http://www.visualroute.com/

03_07 Using nslookup and DIG

- No links

Chapter 4 Conclusion

04_01 Footprinting Countermeasures

- To visit the Wayback machine go to: https://archive.org/web/

04_02 Footprinting Pen Testing and Reports

- For Googles content removal page visit: https://support.google.com/legal/answer/3110420?rd=1

04_03 Summary

- No links