Passive Fingerprinting

Introduction

These are the results of the `Passive Fingerprinting` exercise. This lab is about identifying domains, ip addresses and networks of Compass Security, hereby referred as `target`.

Author

- Knöpfel Daniel

Methodology

I more or less followed the tutorial first, and later i played around a bit with some online tools. Having a purely software developer background, i guess I will need some more time for this.

Exercise Goals

1. list of domains belonging to Compass Security (`target`)
2. list of target hostnames and ip addresses (e.g. www.compass-security.com)
3. list of target ip ranges run by Compass Security
4. list of target ip ranges run by a provider
5. list of target e-mail servers

Results

Domains

The following domains belong to Compass Security

- compass-security.com
- compass-security.ch
- NS1.COMPASS-SECURITY.COM (nameserver)
- NS2.COMPASS-SECURITY.COM (nameserver)
- hacking-lab-ctf.com
- badger.ch
- crl.compass-security.com
- filebox-solution.ch
- filebox-solution.de
- fileboxsolution.ch
- fileboxsolution.com
- fileboxsolution.de
- hacking-lab-ctf.com
- media.compass-security.com
- media.hacking-lab.com
- security-competence.ch
- security-competence.com

- securitycompetence.ch
- urb80-74-140-119.ch-meta.net

Hostnames & IP Addresses

- compass-security.com (incl. www)- 80.74.140.133
- compass-security.ch (incl. www)- 80.74.140.133
- blog.compass-security.com - 80.74.140.132
- NS1.COMPASS-SECURITY.COM - 193.135.215.40 (nameserver)
- NS2.COMPASS-SECURITY.COM - 80.74.140.181 (nameserver)
- https://www.hacking-lab-ctf.com/ - 80.74.140.119
- badger.ch - 80.74.140.119
- crl.compass-security.com
- filebox-solution.ch - 80.74.140.119
- filebox-solution.de
- fileboxsolution.ch
- fileboxsolution.com
- fileboxsolution.de
- hacking-lab-ctf.com - 80.74.140.119
- media.compass-security.com
- media.hacking-lab.com
- security-competence.ch
- security-competence.com - 80.74.154.113
- securitycompetence.ch
- urb80-74-140-119.ch-meta.net

IP ranges owned by Provider

ASN-METANET METANET AG, CH

E-Mail servers

- mx1.compass-security.com
- mx2.compass-security.com

---

additional notes (not really part of the solution)

- compas-security.com and whois info
  - Name server
    - NS1.COMPASS-SECURITY.COM
  - NS2.COMPASS-SECURITY.COM
- Registrar - Infomaniak Network SA - http://www.infomaniak.com - abuse@infomaniak.com / support@infomaniak.ch - 1817347202_DOMAIN_COM-VRSN (Registry Domain ID)