Offensive security lab-report

Moritz Rupp

May 2, 2022

Abstract

This document contains reports about the laboratory of the 5th semester module offensive security.

Contents

1 Lab2

1.1 Exercise 2.2

https://www.hs-albsig.de

$~ nslookup hs-albsig.de
IP: 94.186.153.201

$~ nmap -sC -sV -oA 94.186.153.201
Open ports: 80(HTTP), 443(HTTPS)
Server: nginx 1.16.1
HTTP Version: 1.1

$~ whois hs-albsig
SOA: ns.hs-albsig.de. (141.87.109.5)
Namerserver:

- Nserver: dns1.belwue.de
- Nserver: dns3.belwue.de
- Nserver: dns5.belwue.de
- Nserver: ns.hs-albsig.de 141.87.109.5

$~ fierce –domain hs-albsig –wide
Some of the found subdomains, all belonging to the main host of hs-albsig!
To see the full list, take a look at the file 'fierceoutput.txt'.

- helpdesk.hs-albsig.de. - 141.87.114.175
- info.hs-albsig.de. - 141.87.114.205
- konferenz.hs-albsig.de. - 141.87.115.200
- intern.hs-albsig.de. - 141.87.109.198
- autodiscover.hs-albsig.de. - 141.87.109.198
- h1crelay1.hs-albsig.de. -141.87.109.200
- intranet.hs-albsig.de. - 141.87.109.198
- jobs.hs-albsig.de. - 62.204.161.138
- live.hs-albsig.de. - 141.87.190.3
- login.hs-albsig.de. - 194.98.248.75
- mail.hs-albsig.de. - 141.87.114.190
- mailig.hs-albsig.de. - 54.73.30.56
- ntp.hs-albsig.de. - 141.87.190.5

- pki.hs-albsig.de. - 141.87.109.3
- proxy.hs-albsig.de. - 141.87.109.4
- datascience.hs-albsig.de. - 141.87.109.223

The same results can be achived via recon-ng and the hackertarget module.

$~ recon-ng
$~ marketplace search hackertarget
$~ marketplace install hackertarget
$~ modules load hackertarget
$~ options set SOURCE hs-albsig.de
$~ run

More interesting information about the host hs-albsig.de:
Common http security headers are missing!

- Content-security-policy(csp)
- HTTP Strict Transport Security (HSTS)
- Cross Site Scripting Protection (X-XSS)
- X-Frame-Options
- X-Content-Type-Options(no sniff)

1.2 Exercise 2.3

Out of my 10 email adresses, 3 have been part of a leagage. A paid licence is required to view the actuall document content tho. But it is possible to see the origin of the leagage.
Leagage origins:

- Dailymotion.com
- Dropbox.comment
- Linux-Foren.com
- RepZ.eu
- hqcombo.top

Phonebook.cz was able to find over 500 email adresses of albstadt uni members. The majority of leagages matched the above listing. With the help of tools and websites such as lullar.com, mSpy and peekyou i was able to find the according social media accounts of several email adresses.

1.3 Exercise 2.4

Searching for company related documents with metagoofil:
$~ metagoofil -t pdf -d hs-albsig

Metagoofil found several hundred uni related documents including sensitive files like exams and salary information.
Exemplary scan of one of the found documents with **exiftool**.

```
sleven  parrot  ~/Downloads  exiftool 20220101-Leitlinie_Praesenzpruefungen_INF_Pruefungszeitraum_Februar_2022.pdf
ExifTool Version Number         : 12.16
File Name                       : 20220101-Leitlinie_Praesenzpruefungen_INF_Pruefungszeitraum_Februar_2022.pdf
Directory                       : .
File Size                       : 259 KiB
File Modification Date/Time     : 2022:04:19 13:08:21+02:00
File Access Date/Time           : 2022:04:19 13:08:21+02:00
File Inode Change Date/Time     : 2022:04:19 13:08:29+02:00
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : Yes
Author                          : Knut Kliem
Company                         : Hochschule Albstadt-Sigmaringen
Create Date                     : 2022:01:20 16:58:33+01:00
Modify Date                     : 2022:01:20 16:58:35+01:00
Source Modified                 : D:20220120155822
Language                        : DE-DE
Tagged PDF                      : Yes
XMP Toolkit                     : Adobe XMP Core 7.1-c000 79.425dc87, 2021/10/27-16:20:32
Metadata Date                   : 2022:01:20 16:58:35+01:00
Creator Tool                    : Acrobat PDFMaker 21 für Word
Document ID                     : uuid:aa233347-4851-4e5b-9b58-2a611417e5c7
Instance ID                     : uuid:30302547-31db-4f33-a3cf-5ea5c03d0fa2
Subject                         : 8
Format                          : application/pdf
Creator                         : Knut Kliem
Producer                        : Adobe PDF Library 21.11.71
Page Layout                     : OneColumn
Page Count                      : 4
```

Particular interesting information:
File Size: If much bigger than expected, that could be a sign for more hidden meta data like steganography etc.
File modification/access date/time: Was the file created prior to certain vulnabilities/patches etc.?!
MIME Type: Is the file the format it claims to be?! Executable malware can be hidden as a fake format like pdf or jpg.
Creator: Can be used to ascertain to what department someone belongs to. This can further be used for more osint.
Geotag: If pictures show sensitive infrastrucure of a company(server, admin rooms etc.) the geotag can be used to find the real location. This can be used for stuff like dumbster diving etc.

It can be noticed that most documents didnt include sensitive information such as geotags etc.