THOMAS KRENN®

Linux Security-Tools

Webinar am 30.6.2021

Christoph Mitasch, Thomas-Krenn.AG

THOMAS KRENN®

Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)

LPIC-303, v3

- Thema: Enterprise Security
- v3 dzt. noch Beta Exam
  Online-Prüfung, ohne Test-Center
- https://wiki.lpi.org/wiki/LPIC-303_Objectives_V3.0

Linux Professionals	Open Technology
	
LPIC-1	DevOps Tools Engineer
LPIC-2	BSD Specialist
LPIC-3 Enterprise Mixed Environment	
LPIC-3 Enterprise Security	
LPIC-3 Enterprise Virtualization and High Availability	

Quelle: https://www.lpi.org/

4 Objectives

- 4.1 *Topic 331: Cryptography*
  - 4.1.1 331.1 X.509 Certificates and Public Key Infrastructures (weight: 5)
  - 4.1.2 331.2 X.509 Certificates for Encryption, Signing and Authentication (weight: 4)
  - 4.1.3 331.3 Encrypted File Systems (weight: 3)
  - 4.1.4 331.4 DNS and Cryptography (weight: 5)
- 4.2 *Topic 332: Host Security*
  - 4.2.1 332.1 Host Hardening (weight: 5)
  - 4.2.2 332.2 Host Intrusion Detection (weight: 5)
  - 4.2.3 332.3 Resource Control (weight: 3)
- 4.3 *Topic 333: Access Control*
  - 4.3.1 333.1 Discretionary Access Control (weight: 3)
  - 4.3.2 333.2 Mandatory Access Control (weight: 5)
- 4.4 *Topic 334: Network Security*
  - 4.4.1 334.1 Network Hardening (weight: 4)
  - 4.4.2 334.2 Network Intrusion Detection (weight: 4)
  - 4.4.3 334.3 Packet Filtering (weight: 5)
  - 4.4.4 334.4 Virtual Private Networks (weight: 4)
- 4.5 *Topic 335: Threats and Vulnerability Assessment*
  - 4.5.1 335.1 Common Security Vulnerabilities and Threats (weight: 2)
  - 4.5.2 335.2 Penetration Testing (weight: 3)

Agenda

- Penetration Testing
- Port-Scanning und Netzwerk-Sniffing
- Verschlüsselung Datenträger
- Server Hardening
- Intrusion Detection
- Malware- und File-Integrity-Checker
- Apparmor und SELinux

Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

Intrusion Detection

Malware- und File-Integrity-Checker

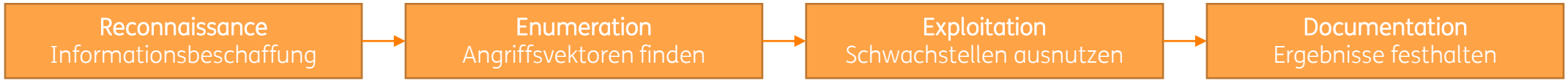
Apparmor und SELinux

Penetration Testing

1.3 Begriffsbestimmung IS-Penetrationstest

Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.

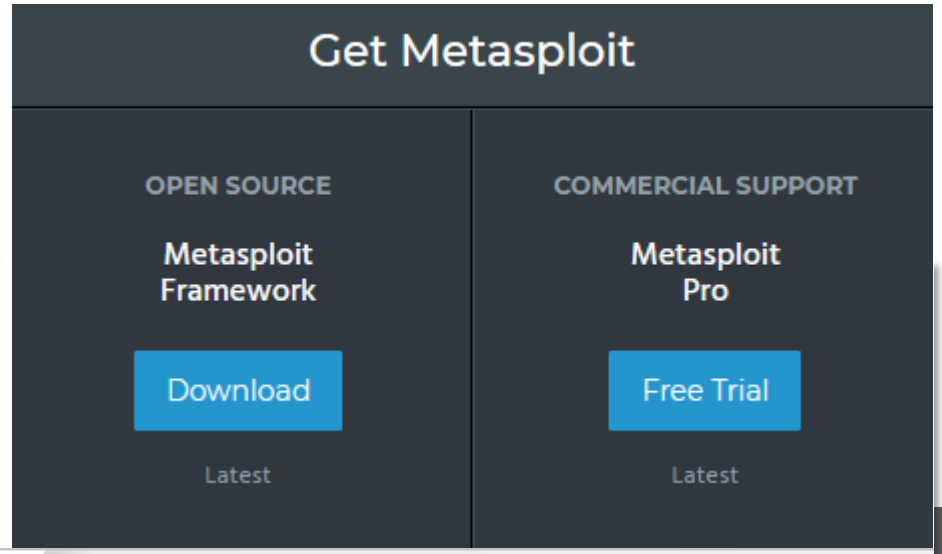
- Praxis-Leitfaden für IS-Penetrationstests
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf
- Mögliche Phasen:

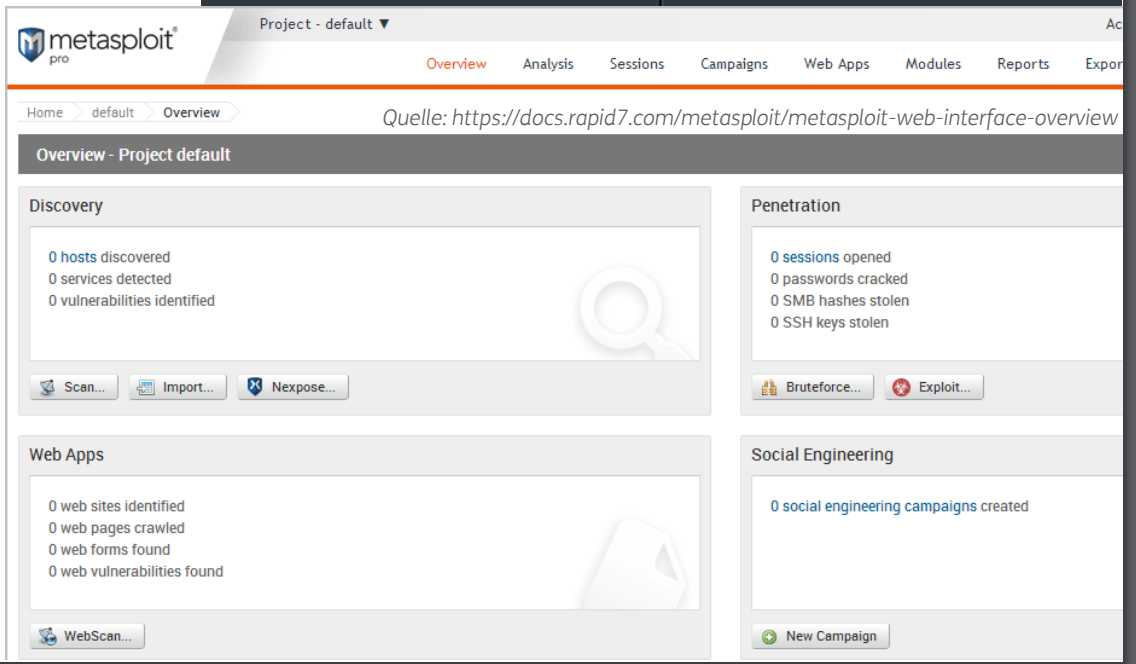


- Rechtliche Aspekte
  - Zustimmung der getesteten Organisation unbedingt vorab notwendig!

Metasploit

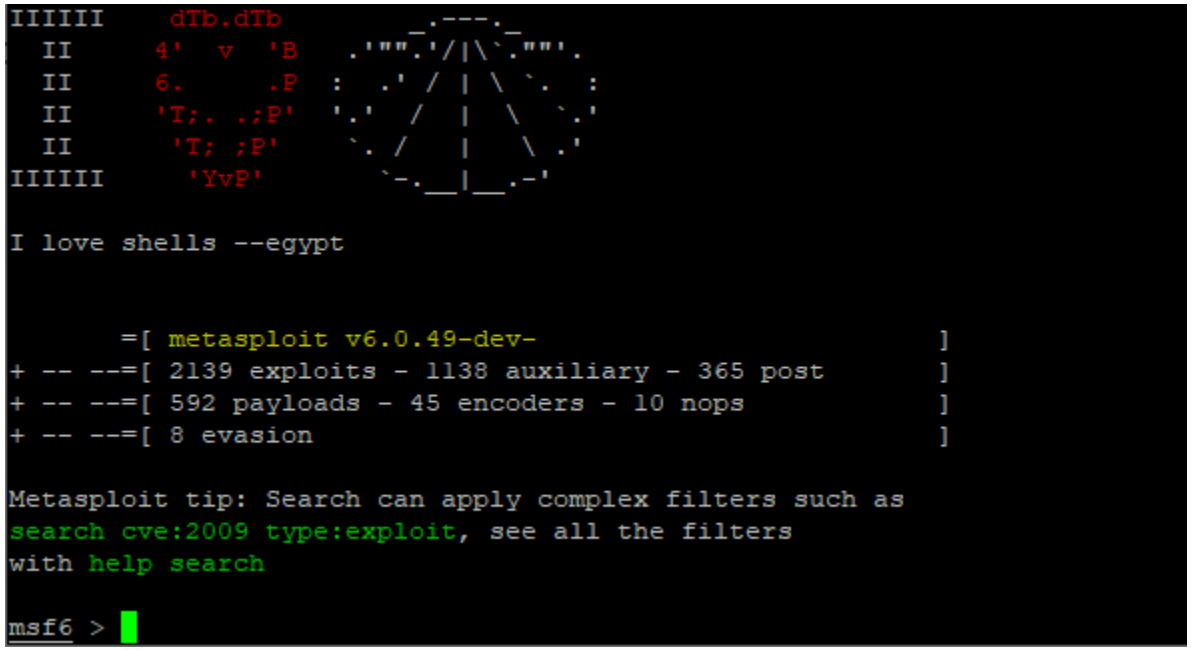
- Installation
  https://computingforgeeks.com/install-metasploit-framework-on-debian/
- msfconsole
  - search
  - use windows/iis/iis_webdav_upload_asp
  - show options
  - set RHOSTS example.com
  - run / exploit
  - show payload
  - set payload payload/generic/shell_reverse_tcp
- Zusätzliche Module integrierbar, z.B. https://www.exploit-db.com/





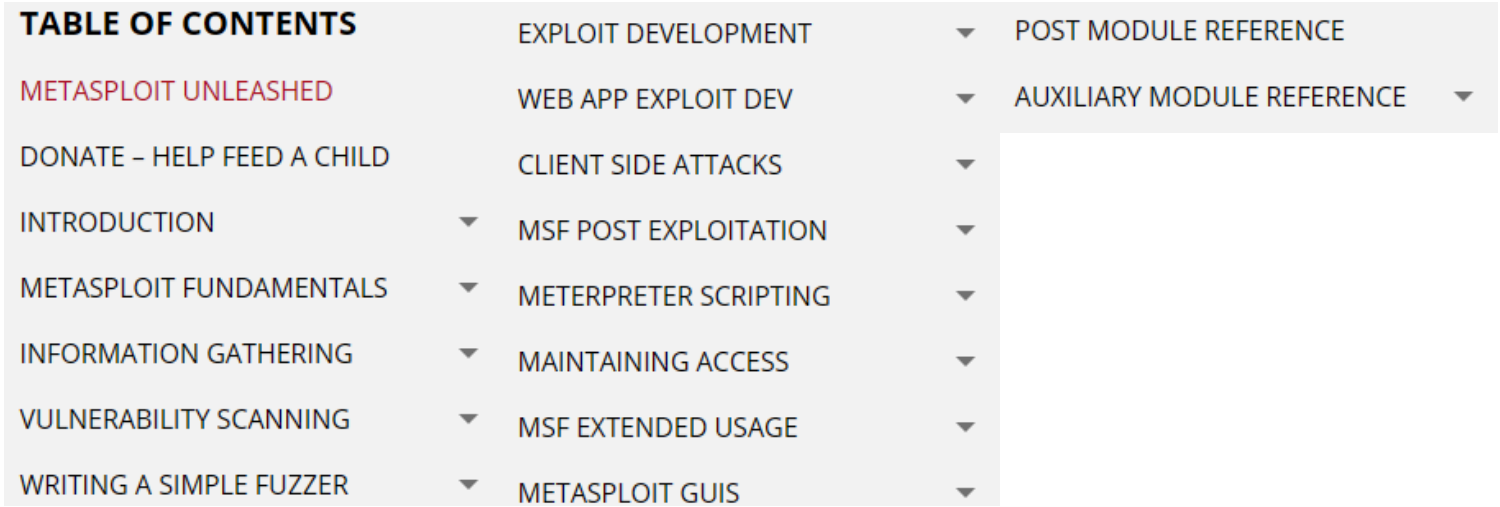
Quelle: https://docs.rapid7.com/metasploit/metasploit-web-interface-overview

Metasploit Demo



Metasploit Details

- auch für Reconnaissance/Enumeration verwendbar mit „auxiliary“ Modulen
- kann auch Port-Scanning, Passwort-Sniffing, u.v.m.
- Module können auch selbst geschrieben und angepasst werden
- https://www.offensive-security.com/metasploit-unleashed/



Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

Intrusion Detection

Malware- und File-Integrity-Checker

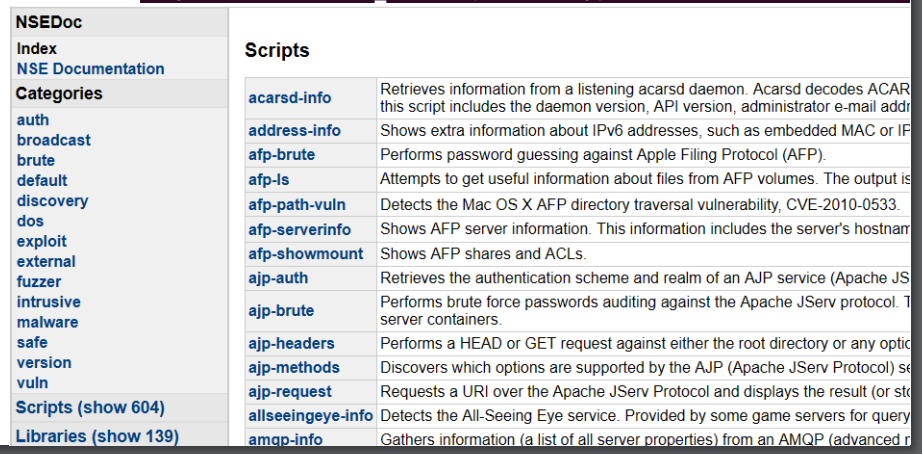
Apparmor und SELinux

Port-Scanning

- nmap - „network mapper“
  - -sT … TCP /-sU … UDP / -sS … SYN / -sF … FIN / -sN … keine Flag
  - -sX … Xmas scan
    - sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree ;)
  - -sn … ping Scan
  - -O … OS detection
  - -sV … service version info
  - -T … timing, 0=paranoid, 4=aggressive
  - --top-ports <number> … scan <number> most common ports
    - laut Liste /usr/share/nmap/nmap-services
  - für viele Scans sind „root“-Rechte notwendig
  - Nmap Scripting Engine (NSE)
    - LUA-Code
    - https://nmap.org/nsedoc/index.html

```
christoph@ubuntu:~$ nmap -sn 10.0.0.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-16 14:49 CEST
Nmap scan report for 10.0.0.4
Host is up (0.00019s latency).
Nmap scan report for 10.0.0.51
Host is up (0.0029s latency).
Nmap scan report for 10.0.0.66
Host is up (0.0061s latency).
Nmap scan report for 10.0.0.67
Host is up (0.020s latency).
Nmap scan report for 10.0.0.69
Host is up (0.021s latency).
Nmap scan report for 10.0.0.76
Host is up (0.022s latency).
Nmap scan report for 10.0.0.138
Host is up (0.0041s latency).
Nmap scan report for 10.0.0.231
Host is up (0.016s latency).
Nmap scan report for 10.0.0.234
Host is up (0.023s latency).
Nmap done: 256 IP addresses (9 hosts up) scanned in 2.70 seconds
```



NSEDoc

Index
NSE Documentation

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

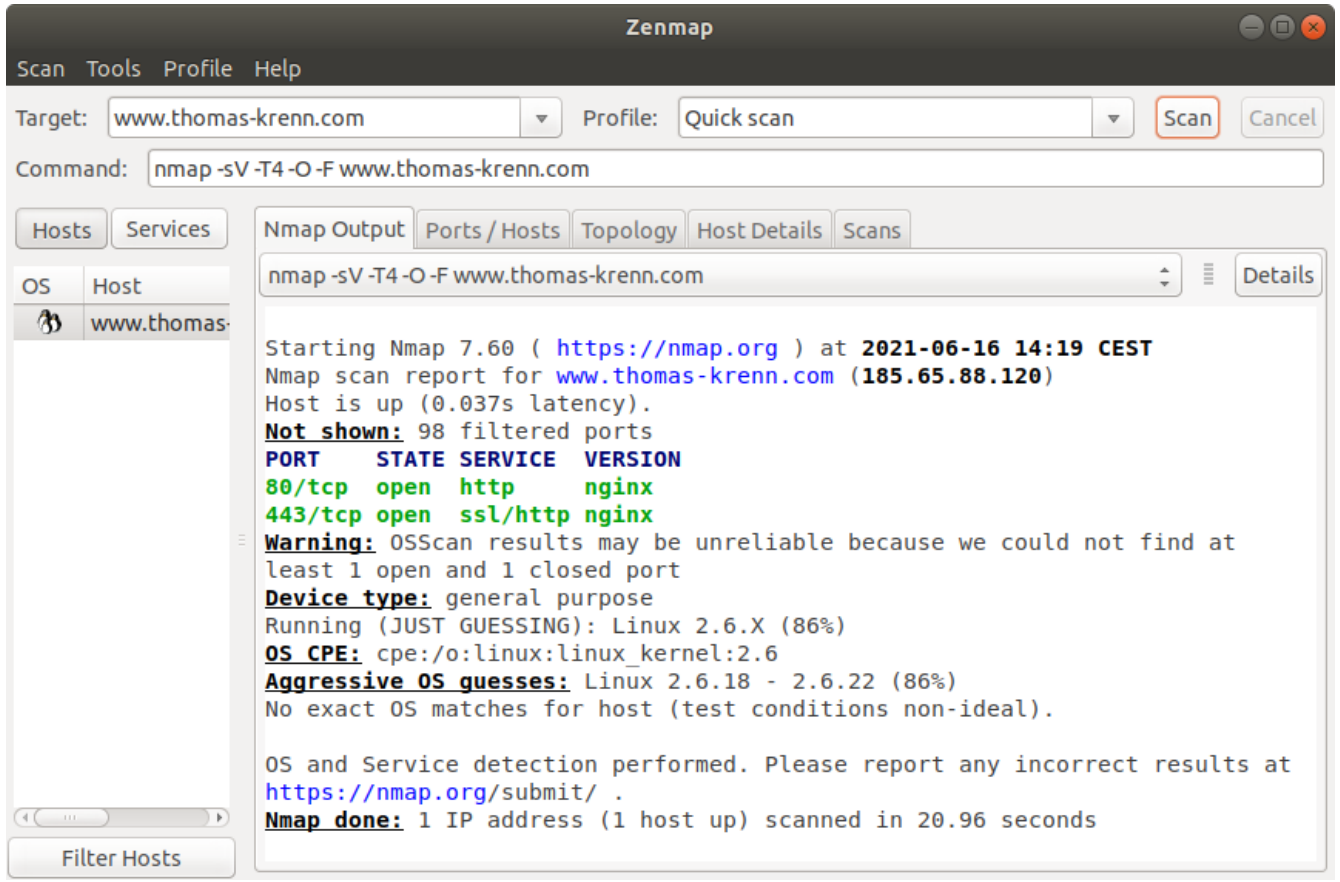
Scripts (show 604)
Libraries (show 139)

Scripts

acarsd-info	Retrieves information from a listening acarsd daemon. Acarsd decodes ACAR this script includes the daemon version, API version, administrator e-mail addr
address-info	Shows extra information about IPv6 addresses, such as embedded MAC or IP
afp-brute	Performs password guessing against Apple Filing Protocol (AFP).
afp-ls	Attempts to get useful information about files from AFP volumes. The output is
afp-path-vuln	Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.
afp-serverinfo	Shows AFP server information. This information includes the server's hostnam
afp-showmount	Shows AFP shares and ACLs.
ajp-auth	Retrieves the authentication scheme and realm of an AJP service (Apache JS
ajp-brute	Performs brute force passwords auditing against the Apache JServ protocol. T server containers.
ajp-headers	Performs a HEAD or GET request against either the root directory or any optic
ajp-methods	Discovers which options are supported by the AJP (Apache JServ Protocol) se
ajp-request	Requests a URI over the Apache JServ Protocol and displays the result (or sto
allseeingeye-info	Detects the All-Seeing Eye service. Provided by some game servers for query
amqp-info	Gathers information (a list of all server properties) from an AMQP (advanced r

Zenmap

- GUI für nmap



Netzwerk Sniffing

- Wireshark
  - Netzwerk-Sniffer GUI
  - verwendet libpcap
  - tshark – für Kommandozeile
  - **Demo**
- tcpdump
  - nur für Kommandozeile
  - verwendet auch libpcap
  - Bsp: **tcpdump -i wlan0 -w output.dump '(tcp port 80) or (tcp port 443)'**
  - Dump kann in Wirekshark GUI geöffnet werden
- ngrep
  - Network Grep
  - Bsp: **ngrep -wi -d any 'user|pass' port 21**
  - **Demo**

Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

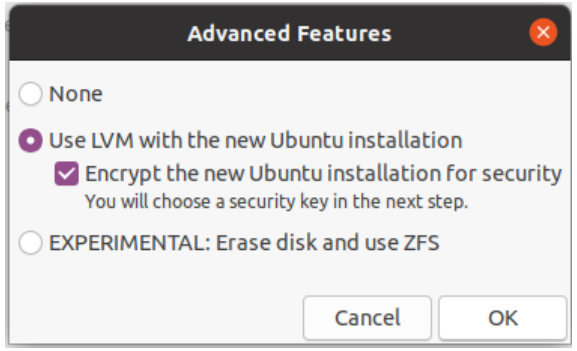
Intrusion Detection

Malware- und File-Integrity-Checker

Apparmor und SELinux

Verschlüsselung Datenträger

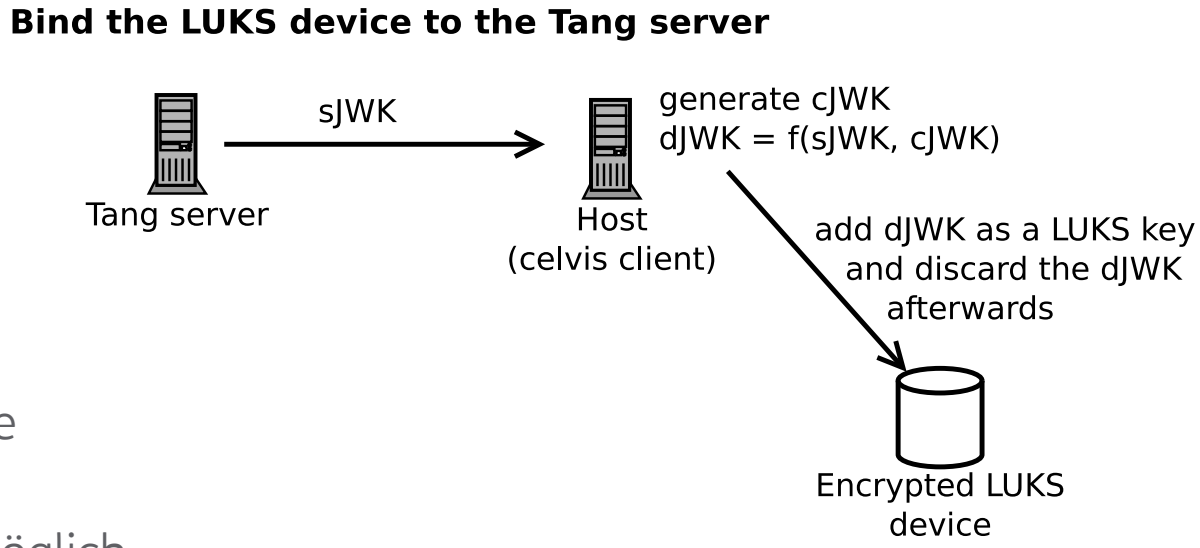
- dm-crypt mit LUKS zur Schlüsselverwaltung, blockbasiert
  - LUKS = Linux Unified Key Setup
  - cryptsetup luksFormat -c aes-xts-plain64 -s 512 -h sha512 /dev/sdX2
  - cryptsetup luksOpen /dev/sdX2 enc_device
  - mkfs.ext4 /dev/mapper/enc_device
  - mount /dev/mapper/enc_device
  - /etc/crypttab für Persistenz
  - Passphrase muss beim Bootvorgang eingegeben werden
  - Ubuntu 20.04 Installer nur zusammen mit LVM




```
cryptsetup -v status enc_device
/dev/mapper/enc_device is active.
  type:    LUKS2
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device:  /dev/loop0
  loop:    /root/100M
  sector size:  512
  offset:  32768 sectors
  size:    172032 sectors
  mode:    read/write
Command successful.
```

Network Bound Disc Encryption (NBDE)

- Tang-Server und Clevis Client notwendig
- interagiert mit LUKS/dm-crypt
- Tang-Server hat Public Key
- Client hat Private Key
- Kombination führt zu LUKS-Key
- Automatische Entschlüsselung ohne Eingabe der Passphrase
- auch für root-Device via „clevis-initramfs“ möglich
- via FIDO2, TPM2 und PKCS#11
  http://0pointer.net/blog/unlocking-luks2-volumes-with-tpm2-fido2-pkcs11-security-hardware-on-systemd-248.html



Quelle: https://semanticlab.net/sysadmin/encryption/Network-bound-disk-encryption-in-ubuntu-20.04/

Ecryptfs

- dateibasierte Verschlüsselung
- per User-Verzeichnis (Bsp: /home/.ecryptfs/christoph/.Private/)
- FNEK (File Name Encryption Key) – verschlüsselt zusätzlich Dateinamen
- Seit Ubuntu 18.04 nicht mehr im Installer dabei
  Paket ist in „universe“-Repo
  -> empfohlen wird FDE (full disk encryption) mit dm-crypt
- „fscrypt“ für ext4 ist Alternative

eCryptfs

The enterprise cryptographic filesystem for Linux

Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

Intrusion Detection

Malware- und File-Integrity-Checker

Apparmor und SELinux

Server Hardening

- BIOS Passwortschutz
- GRUB Bootloader
  - Bootvorgang selbst schützen (Option „--unrestricted“ entfernen)
  - nur Änderungen der Menüeinträge schützen (Option „--unrestricted“ notwendig)
  - Per Default Plaintext Passwörter
    -> **grub-mkpasswd-pbkdf2** (Password-Based Key Derivation Function 2)
  - /etc/grub.d/40_custom
    ```
    set superusers="admin"
    password_pbkdf2 admin grub.pbkdf2.sha512.10000.FC58373BCA15A797C418C1EA7FFB007BF5A5
    ```
  - https://help.ubuntu.com/community/Grub2/Passwords

It is worth repeating: Users experimenting with GRUB 2 passwords should keep at least one non-protected menuentry and set the timeout to at least 1 second until testing is complete. This will allow booting a menuentry without a password to correct problematic settings.

systemd

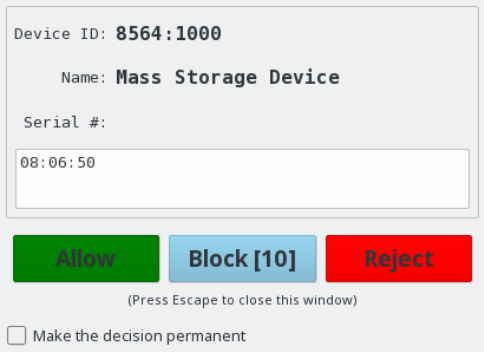
- Capabilities
  - z.B.: CapabilityBoundingSet=CAP_CHOWN CAP_KILL
- Resource Limits
  - z.B.: LimitNPROC … ulimit –u, LimitNOFILE … ulimit –n
- Netzwerk-Isolierung
  - PrivateNetwork=yes … nur Loopback
- Verzeichnisse verbieten, read-only, privates /tmp
  - InaccessibleDirectories=/home, ReadOnlyDirectories=/var
  - PrivateTmp=yes
- Chroot
  - RootDirectory=/chroot/
- /dev-Zugriff einschränken
  - DeviceAllow=/dev/null rw … nur /dev/null, keine anderen Geräte


```
...
[Service]
ExecStart=...
InaccessibleDirectories=/home
ReadOnlyDirectories=/var
...
```

Quelle: http://0pointer.de/blog/projects/security.html

USBguard

- nur angeschlossenen Geräte erlaubt
  `usbguard generate-policy > rules.conf`
- weitere Geräte erlauben
  `usbguard list-devices`
  `usbguard allow-device --permanent 29`
- GUI „*usbguard-applet-qt*“



- https://www.privacy-handbuch.de/handbuch_91a.htm

Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

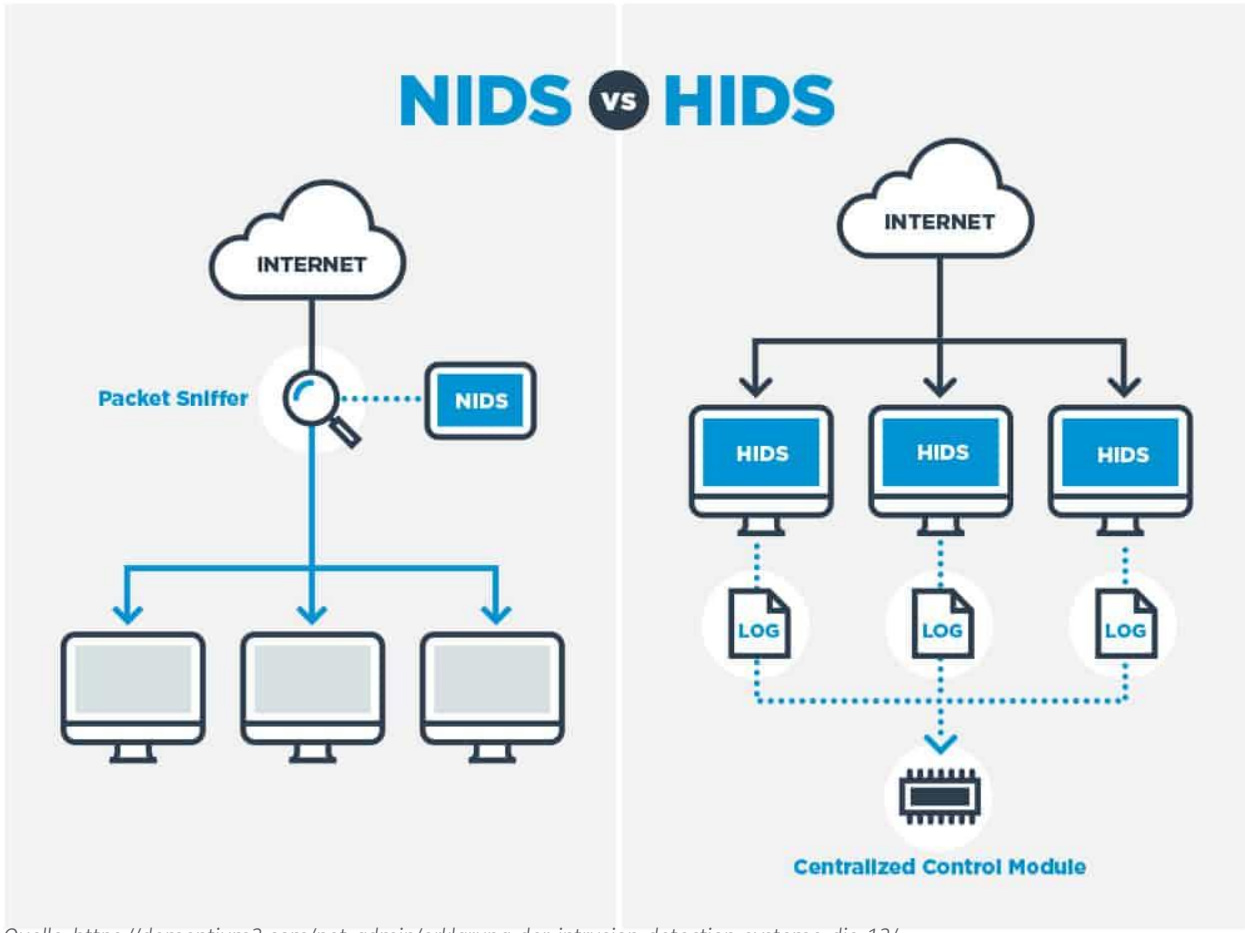
Intrusion Detection

Malware- und File-Integrity-Checker

Apparmor und SELinux

IDS / IPS

- Detection vs. Prevention
- HIDS … Hostbased Intrustion Detection
  - OSSEC, Wazuh (Fork)
  - Fail2ban (Prevention)
    - kann Ergebnisse von OpenVAS verfälschen, daher Whitelist sinnvoll
- NIDS … Networkbased Intrusion Detection
  - Snort
  - Suricata (in OPNsense integriert)



Quelle: https://dementium2.com/net-admin/erklarung-der-intrusion-detection-systeme-die-12/

Snort

- GPL
- 3 Modi:
  - 1. Sniffer, 2. Packet Logger, 3. NIDS
- Regeln:
  - Community (Subset von Subscriber Ruleset)
  - Registered Users (30 Tage später)
  - Subscribed Users (Echtzeit, kostenpflichtig)
- /etc/snort/snort.conf

```
HOME_NET ='10.0.0.0/24'
EXTERNAL_NET = '!$HOME_NET'
```

- Doku: https://snort.org/documents
- in vielen kommerziellen Produkten eingebaut (z.b. VMware NSX, Sophos UTM)

OpenVAS

OpenVAS

Open Vulnerability Assessment Scanner

- Vulnerability Scanner
- Fork von Nessus (2007)
- OpenVAS Scanner ist OpenSource
- Teil von „Greenbone Security Manager" (GSM, kommerziell)
  Greenbone Networks GmbH in Osnabrück
- 2 Feeds:
  - Greenbone Community Feed (GCF), ca. 80.000 Schwachstellen
  - Greenbone Security Feed (GSF), > 94.000 Schwachstellen
- Trial als OVA downloaden- https://www.greenbone.net/jetzttesten/
  - Community Feed
  - kann nicht aktualisiert werden, man muss auf neues OVA warten
  - Daten können nicht übernommen werden, nicht für Dauerbetrieb sinnvoll

OpenVAS

- eigene Erfahrungen waren sehr gut
  -> veraltete Software gefunden, für die sich niemand zuständig fühlte

Schwachstelle	Schweregrad ▼	QdE
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	7.5 (Hoch)	80 %
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	7.5 (Hoch)	80 %
Apache Tomcat HTTP Request Smuggling Vulnerability - Feb20 (Windows)	5.8 (Mittel)	80 %
Apache Tomcat HTTP Request Smuggling Vulnerability - Feb20 (Windows)	5.8 (Mittel)	80 %
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Mittel)	80 %
Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows)	5.0 (Mittel)	80 %
Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows)	5.0 (Mittel)	80 %
Apache Tomcat DoS Vulnerability - June20 (Windows)	5.0 (Mittel)	80 %
Apache Tomcat DoS Vulnerability - June20 (Windows)	5.0 (Mittel)	80 %
SSL/TLS: Report Weak Cipher Suites	5.0 (Mittel)	98 %
Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows	5.0 (Mittel)	80 %
Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows	5.0 (Mittel)	80 %
Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows)	5.0 (Mittel)	80 %
Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows)	5.0 (Mittel)	80 %
FTP Unencrypted Cleartext Login	4.8 (Mittel)	70 %
FTP Unencrypted Cleartext Login	4.8 (Mittel)	70 %
Apache Tomcat RCE Vulnerability - May20 (Windows)	4.4 (Mittel)	80 %
Apache Tomcat RCE Vulnerability (Mar21) - Windows	4.4 (Mittel)	80 %
Apache Tomcat RCE Vulnerability - May20 (Windows)	4.4 (Mittel)	80 %
Apache Tomcat RCE Vulnerability (Mar21) - Windows	4.4 (Mittel)	80 %
Apache Tomcat Information Disclosure Vulnerability - Jan21 (Windows)	4.3 (Mittel)	80 %
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Mittel)	98 %
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Mittel)	98 %

OpenVAS

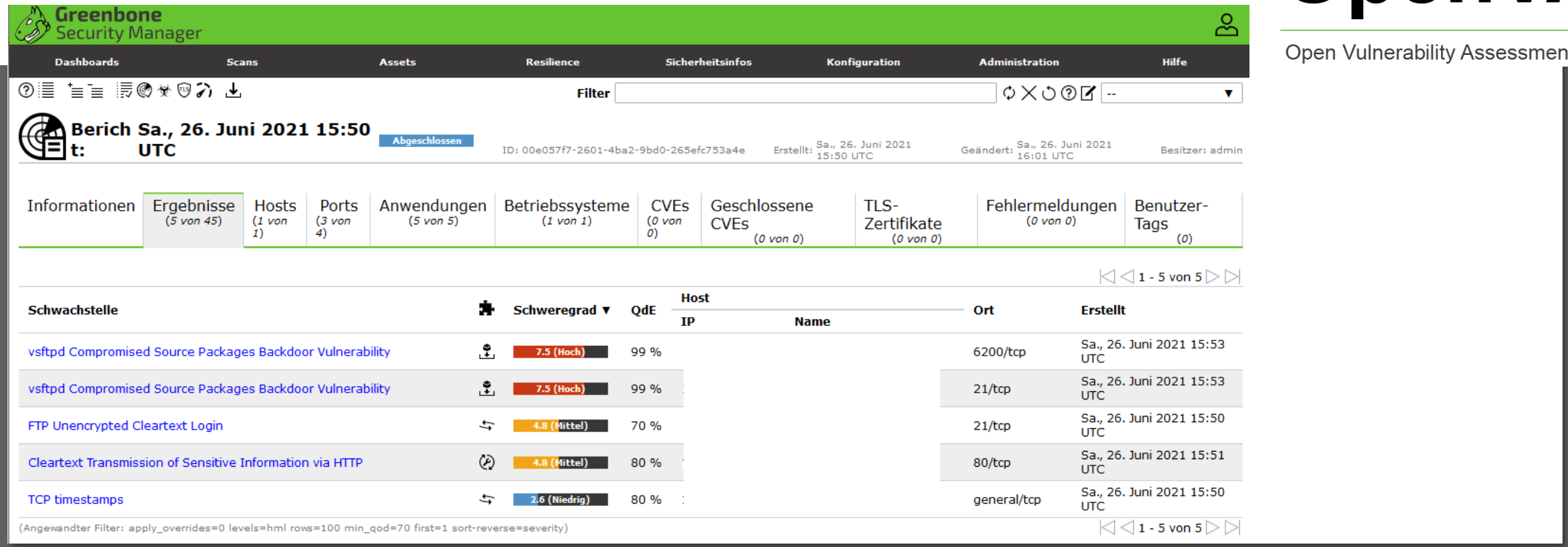
Open Vulnerability Assessment Scanner

OpenVAS

OpenVAS

Open Vulnerability Assessment Scanner

- VSFTD Backdoor der Metasploit Demo wurde auch gefunden



Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

Intrusion Detection

Malware- und File-Integrity-Checker

Apparmor und SELinux

Malware-Checker

- chkrootkit
  - 3000 Zeilen Bash-Script
  - ca. 122 Checks
  - /etc/chkrootkit.conf
  - Cron-Einbindung

```
0 3     * * *   root    (cd /usr/sbin; ./chkrootkit 2>&1 |
mail -s "chkrootkit output" xy@example.com)
```

```
root@buster:~# cat /etc/chkrootkit.conf
RUN_DAILY="false"
RUN_DAILY_OPTS="-q"
DIFF_MODE="false"
```

- rkhunter
  - Alternative zu chkrootkit, mehr Checks
  - /etc/rkhunter.conf

```
[04:44:33]   Checking if SSH root access is allowed          [ Warning ]
[04:44:33] Warning: The SSH configuration option 'PermitRootLogin' has not been set.
           The default value may be 'yes', to allow root access.
[04:44:33]   Checking if SSH protocol v1 is allowed          [ Not set ]
```

```
  Performing system configuration file checks
    Checking for an SSH configuration file                   [ Found ]
    Checking if SSH root access is allowed                   [ Warning ]
    Checking if SSH protocol v1 is allowed                   [ Not set ]
    Checking for other suspicious configuration settings     [ None found ]
    Checking for a running system logging daemon             [ Found ]
    Checking for a system logging configuration file         [ Found ]
    Checking if syslog remote logging is allowed             [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                  [ Warning ]

    Checking for hidden files and directories                [ None found ]

[Press <ENTER> to continue]


System checks summary
=====================

File properties checks...
    Files checked: 142
    Suspect files: 3

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 46 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Malware-Checker

- Linux Malware Detect (LMD)
  - GPL, kostenlos, aktives Projekt
  - nicht in Repo der Distros dabei
  - eigene Signaturen (~17.000)
    - Network Edge IPS
    - Community Data
    - ClamAV (muss aktiviert werden, macht LMD langsamer)
    - User Submission
  - für Webhosting optimiert
  - Inotify-Integration
  - Reports per Email
  - Apache mod_security2 Upload-Scanning
  - Kommando: **`maldet`**
    Konfiguration: **`conf.maldet`**
    Reports: **`/usr/local/maldetect/sess/`**

```
maldet(27669): {sigup} new signature set 202106191172186 available
maldet(27669): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-sigpack.tgz
maldet(27669): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-cleanv2.tgz
maldet(27669): {sigup} verified md5sum of maldet-sigpack.tgz
maldet(27669): {sigup} unpacked and installed maldet-sigpack.tgz
maldet(27669): {sigup} verified md5sum of maldet-clean.tgz
maldet(27669): {sigup} unpacked and installed maldet-clean.tgz
maldet(27669): {sigup} signature set update completed
maldet(27669): {sigup} 17258 signatures (14436 MD5 | 2039 HEX | 783 YARA | 0 USER)
```

File-Integrity-Checker

- Boardmittel
  - rpm –V <Packetname>
  - dpkg –V / --verify <Packetname>, debsums
    - /var/lib/dpkg/info/*.md5sums
    - **dpkg –V pulseaudio**
      ??5?????? c /etc/pulse/default.pa
- AIDE [eyd] – Datei/Verzeichnis Checker
  - vergleichbar mit Tripwire
  - Datenbank mit Hashes wird aufgebaut
  - Support für viele Datei-Attribute
    - File type, Permissions, Inode, Uid, Gid, Link name, Size, Block count, Number of links, Mtime, Ctime and Atime
    - Posix ACL, SELinux, XAttrs and Extended file system attributes
  - aide --init, aide --check
  - /etc/aide.conf
  - DB in /var/lib/aide/
  - Reports auch an Syslog

Agenda

Penetration Testing

Port-Scanning und Netzwerk-Sniffing

Verschlüsselung Datenträger

Server Hardening

Intrusion Detection

Malware- und File-Integrity-Checker

Apparmor und SELinux

Apparmor und SELinux

- beide Technologien basieren auf LSM (Linux Security Modules) und setzten auf MAC – Mandatory Access Control
- Apparmor
  - Default in Debian (seit Buster aktiviert), Ubuntu (seit 7.10 aktiviert) und SuSE (zumindest seit SLES12 aktiviert)
    - Zusatzpakete: apparmor-utils, apparmor-profiles
    - aa-* Kommandos
  - basierend auf Pfadnamen, Capabilities, Netzwerk-Einschränkungen, …
  - im Vergleich zu SELinux einfacher zu konfigurieren
  - Modus „complain“, „enforce“ und „audit“ (protokolliert zusätzlich System Calls)
  - aa-unconfined … zeigt Netzwerkdienste an, die nicht von AA kontrolliert werden
  - ps –Z … zeigt AA Status für Prozesse an
  - Profile in /etc/apparmor.d/
  - https://debian-handbook.info/browse/de-DE/stable/sect.apparmor.html

Apparmor

- Apparmor
  - zusätzliche Profile: /usr/share/apparmor/extra-profiles/
  - Beispiel für Samba SMBD
  - für Apache Zusatzmodul „mod_apparmor.so “
    - Paket „libapache2-mod-apparmor“
    - aktiviert AAHatName und AADefaultHatName in Apache Config
  - ACHTUNG: mit Default-Einstellungen schützt Apparmor nur minimal, hier muss man definitiv Hand anlegen!

```
root@buster:/etc/apparmor.d# /sbin/aa-status
apparmor module is loaded.
20 profiles are loaded.
5 profiles are in enforce mode.
   /usr/bin/man
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
15 profiles are in complain mode.
   /usr/sbin/dnsmasq
   /usr/sbin/dnsmasq//libvirt_leaseshelper
   avahi-daemon
   identd
   klogd
   mdnsd
   nmbd
   nscd
   ping
   smbd
   smbldap-useradd
   smbldap-useradd///etc/init.d/nscd
   syslog-ng
   syslogd
   traceroute
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```

```
root@buster:/etc/apparmor.d# cat usr.sbin.smbd
#include <tunables/global>

profile smbd /usr/{bin,sbin}/smbd flags=(complain) {
  #include <abstractions/authentication>
  #include <abstractions/base>
  #include <abstractions/consoles>
  #include <abstractions/cups-client>
  #include <abstractions/nameservice>
  #include <abstractions/samba>
  #include <abstractions/user-tmp>
  #include <abstractions/wutmp>

  capability audit_write,
  capability dac_override,
  capability dac_read_search,
  capability fowner,
  capability lease,
  capability net_bind_service,
  capability setgid,
  capability setuid,
  capability sys_admin,
  capability sys_resource,
  capability sys_tty_config,

  /etc/mtab r,
  /etc/netgroup r,
  /etc/printcap r,
  /etc/samba/* rwk,
  @{PROC}/@{pid}/mounts r,
  @{PROC}/sys/kernel/core_pattern r,
  /usr/lib*/samba/vfs/*.so mr,
  /usr/lib*/samba/auth/*.so mr,
  /usr/lib*/samba/charset/*.so mr,
  /usr/lib*/samba/gensec/*.so mr,
  /usr/lib*/samba/pdb/*.so mr,
  /usr/lib*/samba/{lowcase,upcase,valid}.dat r,
  /usr/lib/@{multiarch}/samba/*.so{,.[0-9]*} mr,
  /usr/lib/@{multiarch}/samba/**/ r,
  /usr/lib/@{multiarch}/samba/**/*.so{,.[0-9]*} mr,
```

SELinux

- SELinux
  - von NSA und RedHat entwickelt
  - Standard in RedHat/CentOS
  - in Debian und SLES verfügbar, in Ubuntu schlecht gewartet
  - viel mächtiger aber auch aufwändiger als AppArmor
  - „Bell-LaPadula“ Modell
  - Modi: „enforcing (1)“, „permissive (0)“ und „disabled“
    - Abfrage mit „sestatus“
  - Standard-Regeln: „targeted“ (default) und „strict“ (default Deny)
  - Sicherheitskontext hängt von Benutzer, Rolle und Domain ab
  - Dateien und Prozesse haben einen Kontext
  - SELinux Kontext in Extended Attributes bei Dateien gespeichert, Achtung bei Backup/Restore!
  - https://debian-handbook.info/browse/de-DE/stable/sect.selinux.html

Warning

The Ubuntu-specific "selinux" and "selinux-policy-ubuntu" packages documented here have not received much attention since Karmic, and appear to be effectively broken in Precise.

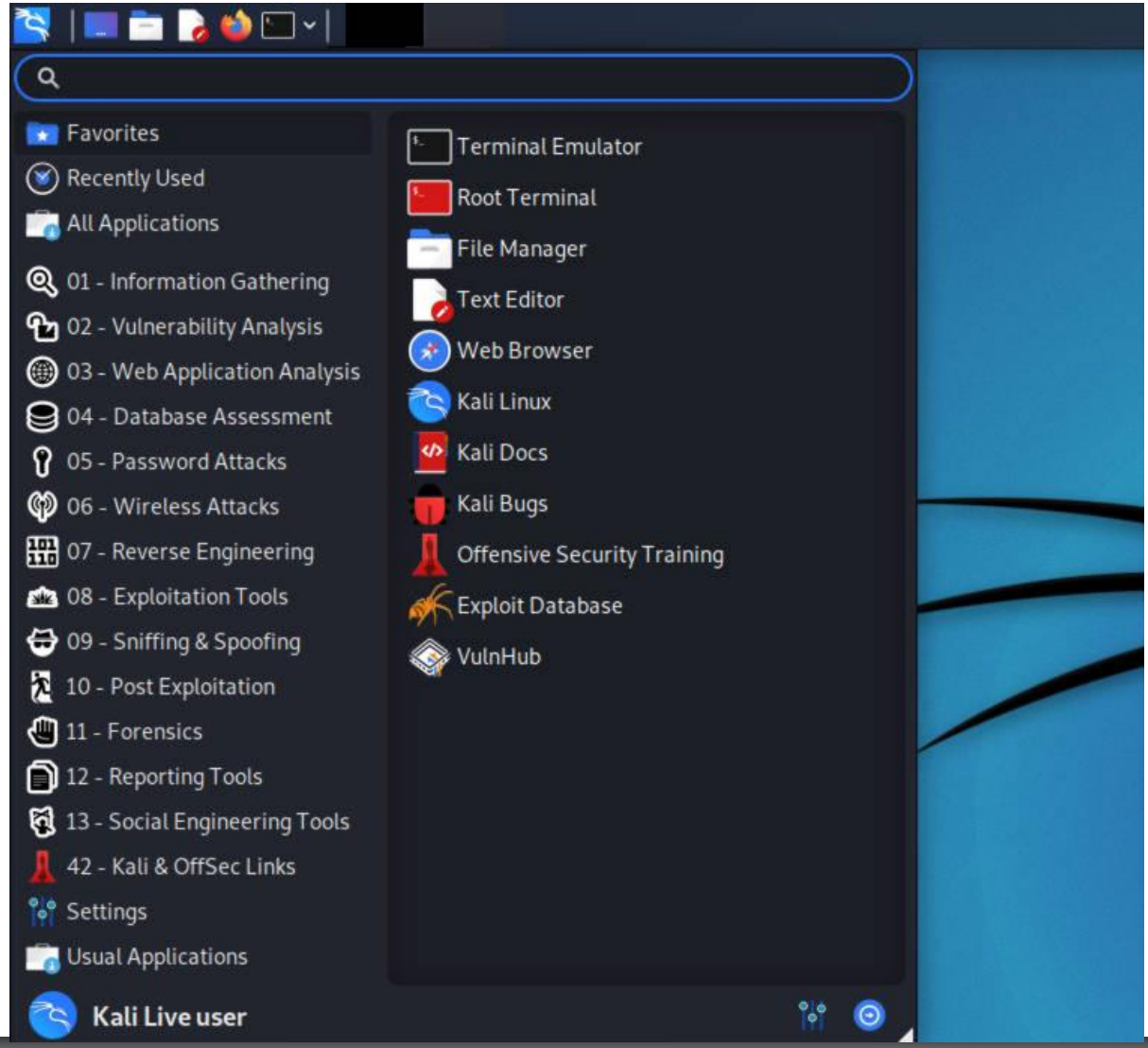
If you wish to use SELinux in Ubuntu, the "selinux-basics" and "selinux-policy-default" packages from Debian are still being actively maintained. Documentation relevant to those packages can be found at http://wiki.debian.org/SELinux

```
$ ls -Z /home/username/myfile.txt
-rw-r--r--  username username user_u:object_r:user_home_t      /home/username/myfile.txt
```

```
$ ps axZ | grep httpd
system_u:system_r:httpd_t       3234 ?        Ss     0:00 /usr/sbin/httpd
```

Tipp: Kali Linux

- eigene Distro für Penetration-Testing und Forensik
- auch als Live-System verfügbar



Quelle: https://www.kali.org/

THOMAS KRENN®

Vielen Dank für Ihre Aufmerksamkeit!