

## **LPIC-3, Prüfung 303**

### 320 Kryptographie

#### 320.1 OpenSSL

Gewichtung: 4

Beschreibung:

Kandidaten sollten OpenSSL konfigurieren und benutzen können. Dies beinhaltet die Erstellung einer eigenen Zertifizierungsstelle (CA) und das Ausstellen von SSL Zertifikaten für verschiedene Anwendungen

Wichtigste Wissensgebiete:

- \* Generierung von Zertifikaten
- \* Generierung von Schlüsseln
- \* SSL/TLS Klient- und Servertests

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* openssl
- \* RSA, DH und DSA
- \* SSL
- \* X.509
- \* CSR
- \* CRL

#### 320.2 Fortgeschrittene Benutzung von GPG

Gewichtung: 4

Beschreibung:

Kandidaten sollten GPG benutzen können. Dies beinhaltet die Erstellung von Schlüsseln, Signierung und Veröffentlichung an einen Schlüsselserver, sowie

die Verwaltung mehrerer privater Schlüssel und IDs

Wichtigste Wissensgebiete:

- \* GPG Verschlüsselung und Signierung
- \* Verwaltung privater und öffentlicher Schlüssel
- \* GPG Schlüsselservers
- \* GPG Konfiguration

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* gpg
- \* gpgv
- \* gpg-agent
- \* ~/.gnupg/

## 320.3 Verschlüsseln von Dateisystemen

Gewichtung: 3

Beschreibung:

Kandidaten sollten in der Lage sein, verschlüsselte Dateisysteme zu erstellen und konfigurieren

Wichtigste Wissensgebiete:

- \* LUKS
- \* dm-crypt und Wissen von CBC, ESSIV, LRW, und XTS Modi

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* dm-crypt
- \* cryptmount
- \* cryptsetup

## 321 Zugriffskontrolle

### 321.1 Hostbasierte Zugriffskontrolle

Gewichtung: 2

Beschreibung:

Kandidaten sollten mit den grundlegenden, hostbasierten Zugriffskontrollmechanismen

wie z.B. der Konfiguration von nsswitch und PAM sowie Password-Cracking vertraut sein.

Wichtigste Wissensgebiete:

- \* PAM und PAM-Konfigurationsdateien
- \* Password Cracking
- \* nsswitch

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* nsswitch.conf
- \* john

### 321.2 Erweiterte Attribute (Extended Attributes) und ACLs

Gewichtung: 5

Beschreibung:

Kandidaten müssen Extended Attributes und ACLs verstehen und benutzen können.

Wichtigste Wissensgebiete:

- \* ACLs
- \* EAs und Attributklassen

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* getfacl
- \* setfacl
- \* getfattr
- \* setfattr

### 321.3 SELinux

Gewichtung: 6

Beschreibung:

Kandidaten sollten genaue Kenntnisse über SELinux besitzen

Wichtigste Wissensgebiete:

- \* SELinux Konfiguration und Werkzeuge auf der Kommandozeile
- \* TE, RBAC, MAC Konzepte und ihre Benutzung

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* fixfiles/setfiles
- \* newrole
- \* setenforce/getenforce
- \* selinuxenabled
- \* semanage
- \* sestatus
- \* /etc/selinux/
- \* /etc/selinux.d/

## 321.4 Andere Systeme zur Mandatory Access Control

Gewichtung: 2

Beschreibung:

Kandidaten sollten mit anderen Mandatory Access Control Systemen vertraut sein. Dies beinhaltet wesentliche Features dieser Systeme aber nicht ihre Konfiguration

Wichtigste Wissensgebiete:

- \* SMACK
- \* AppArmor

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* SMACK
- \* AppArmor

## 322 Sicherheit auf Applikationsebene i

### 322.1 BIND/DNS

Gewichtung: 2

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung von BIND-DNS Diensten haben

Wichtigste Wissensgebiete:

- \* Bind v9

- \* BIND Sicherheitslücken
- \* chroot Umgebungen

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* TSIG
- \* BIND ACLs
- \* named-checkconf

## 322.2 Konzepte

Gewichtung: 2

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung von Postfix Mailediensten haben. Wissen über Sicherheitsaspekte bei sendmail wird auch vorausgesetzt, nicht jedoch die Konfiguration von sendmail

Wichtigste Wissensgebiete:

- \* Auf Sicherheit bedachte Konfiguration von sendmail
- \* Absichern von Sendmail
- \* chroot Umgebungen

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* /etc/postfix
- \* TLS

## 322.3 Apache/HTTP/HTTPS

Gewichtung: 2

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung des Apache Web-Dienstes haben

Wichtigste Wissensgebiete:

- \* Auf Sicherheit bedachte Konfiguration von apache v1 und v2

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* SSL
- \* .htaccess
- \* Basic Authentication
- \* htpasswd
- \* AllowOverride

## 322.4 FTP

Gewichtung: 1

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung des pure-ftpd und vsftpd FTP-Dienste haben

Wichtigste Wissensgebiete:

- \* Pure-FTPd und wichtige Kommandozeilenoptionen
- \* vsftpd Konfiguration
- \* chroot Umgebungen

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* SSL/TLS
- \* vsftp.conf

## 322.5 OpenSSH

Gewichtung: 3

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung der OpenSSH SSH-Dienste

Wichtigste Wissensgebiete:

- \* OpenSSH Konfiguration und Tools auf der Kommandozeile
- \* OpenSSH Schlüsselverwaltung und Zugriffskontrolle
- \* Wissen von Sicherheitsaspekten der SSH-Protokolle v1 und v2

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* /etc/ssh/
- \* ~/.ssh/

- \* ssh-keygen
- \* ssh-agent
- \* ssh-vulnkey

## 322.6 NFSv4

Gewichtung: 1

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung von NFSv4 NFS-Diensten haben. Kenntnisse über vorhergehende Versionen von NFS werden nicht vorausgesetzt.

Wichtigste Wissensgebiete:

- \* NFSv4 Verbesserungen bezüglich Sicherheit, derzeitige Schwachstellen und Benutzung
- \* NFSv4 pseudo Dateisystem
- \* NFSv4 Sicherheitsmechanismen (LIPKEY, SPKM, Kerberos)

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* NFSv4 ACLs
- \* nfs4acl
- \* RPCSEC\_GSS
- \* /etc/exports

## 322.7 Syslog

Gewichtung: 1

Beschreibung:

Kandidaten sollten Erfahrungen und Kenntnisse über Sicherheitsaspekte bei der Konfiguration und Benutzung von syslog-Diensten haben.

Wichtigste Wissensgebiete:

- \* Sicherheitsaspekte von syslog
- \* chroot Umgebungen

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* entfernte syslog Server

## 323 Sicherheit während des Betriebs

### 323.1 Verwaltung von Hostkonfigurationen

Gewichtung: 2

Beschreibung:

Kandidaten sollten mit der Benutzung von RCS und Puppet zur Verwaltung von Hostkonfigurationen vertraut sein.

Wichtigste Wissensgebiete:

- \* RCS
- \* Puppet

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* RCS
- \* ci/co
- \* rcsdiff
- \* puppet
- \* puppetd
- \* puppetmasterd
- \* /etc/puppet/

## 324 Sicherheit im Netzwerk

### 324.1 Intrusion Detection

Gewichtung: 4

Beschreibung:

Kandidaten sollten mit der Benutzung und Konfiguration von Intrusion Detection Software vertraut sein.

Wichtigste Wissensgebiete:

- \* Konfiguration, Regeln und Benutzung von Snort
- \* Konfiguration, Richtlinien und Benutzung von Tripwire

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* snort

- \* snort-stat
- \* /etc/snort
- \* tripwire
- \* twadmin
- \* /etc/tripwire

## 324.2 Sicherheitsscannen von Netzwerken

Gewichtung: 5

Beschreibung:

Kandidaten sollten mit der Benutzung und Konfiguration von Werkzeugen zum Sicherheitsscannen von Netzwerken sein.

Wichtigste Wissensgebiete:

- \* Nessus Konfiguration, NASL und Benutzung
- \* Wireshark Filter und Benutzung

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* nmap
- \* wireshark
- \* tshark
- \* tcpdump
- \* nessus
- \* nessus-adduser/nessus-rmuser
- \* nessusd
- \* nessus-mkcert
- \* /etc/nessus

## 324.3 Netzwerkmonitoring

Gewichtung: 3

Beschreibung:

Kandidaten sollten mit der Benutzung und Konfiguration von Werkzeugen zum Netzwerkmonitoring vertraut sein.

Wichtigste Wissensgebiete:

- \* Nagios Konfiguration und Benutzung

- \* ntop

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* ntop
- \* nagios
- \* nagiosstats
- \* nagios.cfg und andere Konfigurationsdateien

## 324.4 netfilter/iptables

Gewichtung: 5

Beschreibung:

Kandidaten sollten mit der Benutzung und Konfiguration von iptables vertraut sein

Wichtigste Wissensgebiete

- \* iptables Paketfilterung und NAT

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* iptables
- \* iptables-save/iptables-restore

## 324.5 OpenVPN

Gewichtung: 3

Beschreibung:

Kandidaten sollten mit der Benutzung und Konfiguration von OpenVPN vertraut sein.

Wichtigste Wissensgebiete:

- \* OpenVPN Konfiguration und Benutzung

Hier ist eine auszugsweise Liste der verwendeten Dateien, Begriffe und Hilfsprogramme:

- \* /etc/openvpn/
- \* openvpn Server und Klient