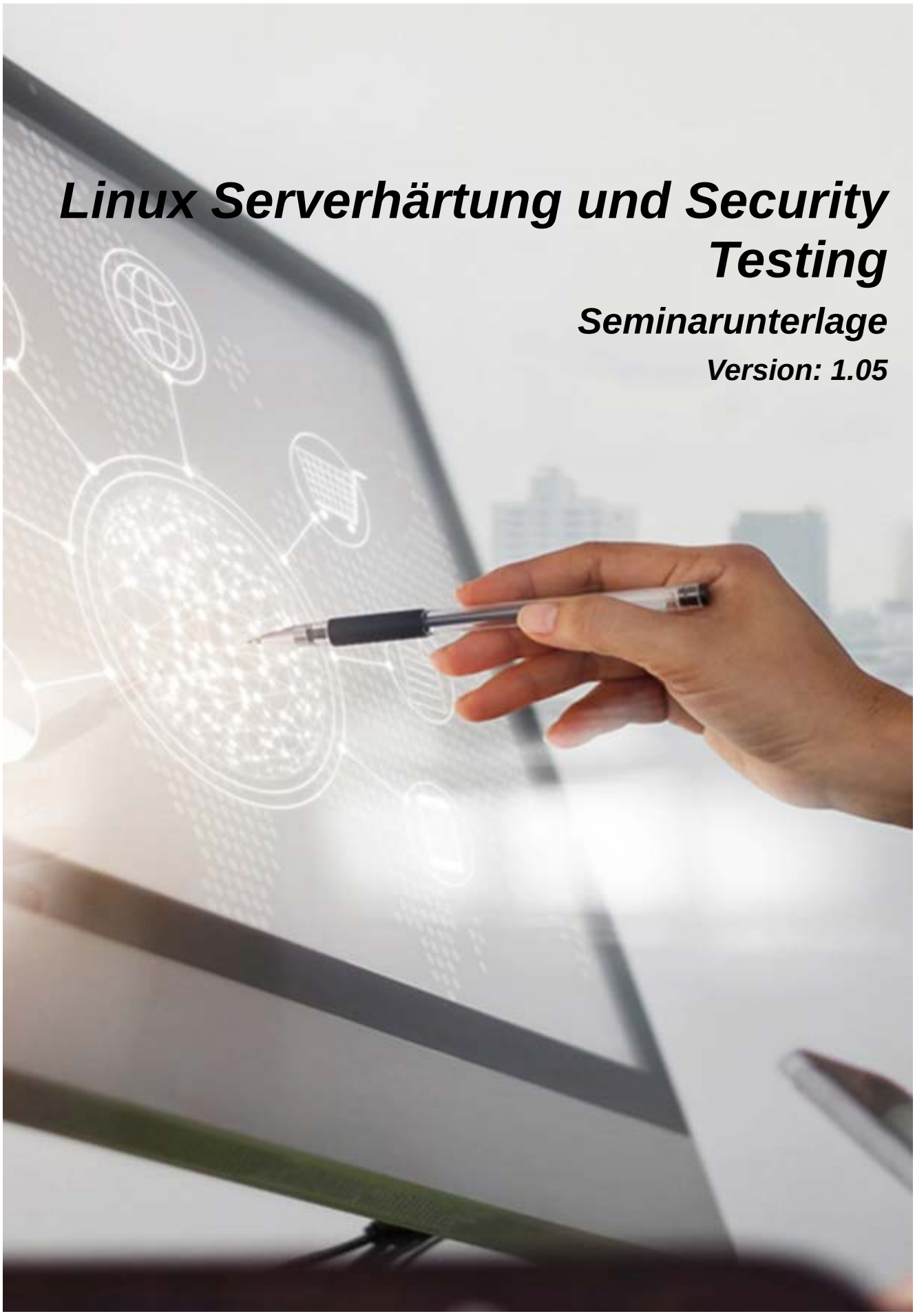

Linux Serverhärtung und Security Testing

Seminarunterlage

Version: 1.05

Version 1.05 vom
30. Januar 2024

Adressen der ORDIX AG

Die ORDIX AG besitzt folgende Geschäftsstellen

ORDIX AG
Karl-Schurz-Straße 19a
D-33100 Paderborn
Tel.: (+49) 0 52 51 / 10 63 - 0
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Kreuzberger Ring 13
D-65205 Wiesbaden
Tel.: (+49) 06 11 / 7 78 40 – 00
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
An der alten Ziegelei 5
D-48157 Münster
Tel.: (+49) 02 51 / 9 24 35 – 00
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Wikingerstraße 18-20
D-51107 Köln
Tel.: (+49) 02 21 / 8 70 61 – 0
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Welser Straße 9
D-86368 Gersthofen
Tel.: (+49) 08 21 / 507 492 – 0
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG
Südwestpark 67/2
D-90449 Nürnberg
Tel.: (+49) 0 52 51 / 10 63 - 0
Fax.: (+49) 01 80 / 1 67 34 90

Internet: http://www.ordix.de

Email: seminare@ordix.de

Inhaltsverzeichnis

1 Anforderungen ... 6

1.1 Schutzziele ... 7
1.2 Vertraulichkeit ... 8
1.3 Verfügbarkeit ... 9
1.4 Integrität ... 10
1.5 Authentizität ... 11
1.6 Nicht-Abstreitbarkeit ... 12
1.7 Aufgaben ... 13

2 Bedrohungen ... 14

2.1 Schadprogramme/Malware ... 15
2.2 Verbreitung ... 16
2.3 Typen ... 17

3 Schwachstellen ... 18

3.1 Übersicht Schwachstellen – Bedrohungen – Risiken ... 19
3.2 DOS ... 20
3.3 DDOS ... 21
3.4 MAC-Flooding ... 22
3.5 Buffer Overflow ... 23
3.6 Spoofing ... 24
3.7 Phishing ... 25
3.8 Man-in-the-Middle ... 26
3.9 OSI-Level 8 ... 27
3.10 Aufgaben ... 28

4 Benutzermanagement ... 29

4.1 Benutzerdatenbank ... 30
4.2 Passwörter ... 31
4.3 Passwortmanagement ... 32
4.4 Rollen und Rechte ... 33
4.5 Privilege Escalation ... 34
4.6 Passwörter raten ... 35
4.7 Aufgaben ... 36

5 Zugriffsrechte ... 37

5.1 Methoden ... 38
5.2 Klassische Rechte ... 39
5.3 Spezial Bits ... 40
5.4 ACL ... 41
5.5 Suche ... 42
5.6 Aufgaben ... 43

6 Netzwerk ... 44

6.1 Einleitung ... 45
6.2 OSI-Schichten ... 46
6.3 Mögliche Absicherung ... 47
6.4 IP Header ... 48
6.5 TCP/IP ... 49
6.6 Detektion offener Ports/Verbindungen ... 50
6.7 Netstat – Der Zustand des Netzwerks ... 51
6.8 ss – Analyse von Sockets ... 52
6.9 Nmap - Portscanner ... 53
6.10 Tcpdump - Paket Sniffer auf der Kommandozeile ... 54
6.11 Wireshark – Grafische Paketanalyse ... 55
6.12 Aufgaben ... 56

7 Verschlüsselung ... 57

7.1 Verschlüsselung ... 58
7.2 Symmetrische Verschlüsselung ... 59
7.3 Blockchiffren ... 60
7.4 Stromchriffren ... 61
7.5 Symmetrische Schlüsselverwaltung ... 62
7.6 Asymmetrisch ... 63
7.7 RSA, DH und Elliptische Kurven ... 64
7.8 Hybride Kryptographie ... 65
7.9 Asymmetrischer Schlüsselaustausch ... 66
7.10 Ablauf RSA ... 67
7.11 Ablauf Diffie Hellmann ... 68
7.12 Hashing ... 69
7.13 Weitere Vorteile durch Kryptographie ... 70
7.14 Vorgehen bei Signaturen ... 71
7.15 Schlüsselverwaltung ... 72
7.16 Aufgaben ... 73

8 Frameworks ... 74

8.1 Übersicht ... 75
8.2 BSI ... 76
8.3 PCI DSS ... 77
8.4 CIS ... 78
8.5 OWASP ... 79

9 OpenSSL ... 80

9.1 Was ist SSL ... 81
9.2 Verbindungsaufbau ... 82
9.3 Netzwerksniffer ... 83
9.4 Protokolle ... 84
9.5 Handshake ... 85
9.6 Ciphersuiten ... 86
9.7 Extensions ... 87
9.8 Ablauf ... 88
9.9 Cipherauswahl ... 89
9.10 Absicherung ... 90
9.11 Aufgaben ... 91

10 OpenSSH ... 92

10.1 Secure Shell ... 93
10.2 Grundbegriffe ... 94
10.3 Sitzungsaufbau ... 95
10.4 Eigenschaften ... 96
10.5 Konfiguration Server ... 97
10.6 Konfiguration Client ... 98
10.7 Keygenerierung ... 99
10.8 Tunnel ... 100
10.9 Absicherung ... 101
10.10 Filetransfer ... 102
10.11 Trust on first use ... 103
10.12 Management der knwon_hosts ... 104
10.13 Host-Key-Signing ... 105
10.14 Host-Key-Signing – CA eintragen ... 106
10.15 KRL – Key-Revocation-List ... 107
10.16 Nützliches ... 108
10.17 User-Key-Signing ... 109
10.18 Aufgaben ... 110

11 Absicherung ... 111

11.1 Absicherung ... 112
11.2 Deinstallieren/deaktivieren ... 113

11.3 Dienste auf Localhost betreiben ... 114
11.4 Ports sperren/filtern ... 115
11.5 Patch-Management ... 116
11.6 Tunnel ... 117
11.7 Zugriffsrechte einschränken ... 118
11.8 SELinux & AppArmor ... 119
11.9 Ressourcen Trennung ... 120
11.10 CVE & CVSS ... 121
11.11 Scanner und Hilfsmittel ... 122
11.12 Aufgaben ... 123

12 Auditing ... 124

12.1 Syslog ... 125
12.2 Kernel Auditing ... 126
12.3 Tripwire ... 127
12.4 Vorgehen ... 128
12.5 Aufgaben ... 129

13 Verfügbarkeit ... 130

13.1 Verfügbarkeit ... 131
13.2 Redundanz ... 132
13.3 Backup ... 133
13.4 Durchführung ... 134

14 Ausblick ... 135

14.1 Tellerrand ... 136
14.2 Weitere Maßnahmen ... 137
14.3 Aufgaben ... 138

15 Lösungen ... 139

15.1 Kapitel 1 ... 140
15.2 Kapitel 3 ... 141
15.3 Kapitel 4 ... 142
15.4 Kapitel 5 ... 147
15.5 Kapitel 6 ... 150
15.6 Kapitel 7 ... 153
15.7 Kapitel 9 ... 154
15.8 Kapitel 10 ... 161
15.9 Kapitel 11 ... 165
15.10 Kapitel 12 ... 170
15.11 Kapitel 14 ... 173