

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
5						
6	1XXX M	Introduction and Legal Stuff				
7	2000.00	L	ASL Discovery. Feel Comfortable with Glocken Emil Shop	Webapp Security	Intro	Intro Vulnerable Hacking-Lab Webapp
8	2100.00	L	User Enumeration - GlockenEmil Username Enumeration	Webapp Security	Authentication Attack	Username Enumeration. Find out valid users in the web app
9	2101.00	L	Authorization - ProfileID Enumeration	Webapp Security	Authorization Bypass	Authorization Bypass and list other users profile
10	2102.00	L	Snoop HTTP Plain Text Passwords	Network Security	Sniffing	Sniffing HTTP Passwords with arp spoofing and wireshark
11	2202.10	L	Snoop Session ID (http)	Network Security	Sniffing	Sniffing HTTP Session when secure flag of cookie is not set
12	2202.20	L	Internet Café and Persistent Cookies (expire flag problem)	Webapp Security	Caching	Exploit persistent cookie (Internet Cafe case)
13	2202.30	L	Session Fixation	Webapp Security	Session Attacks	Get a valid session from the app, let the victim authenticate
14	2202.40	L	Predictable Session-Ids (Extended)	Webapp Security	Session Attacks	curl script for the session prediction algorithm
15	2202.50	L	Predictable Session-Ids (Prepared)	Webapp Security	Session Attacks	curl script for the session prediction algorithm
16	2202.60	L	HTTP link in HTTPS page problem (secure flag problem)	Webapp Security	Sniffing	Exploit missing secure flag in cookie settings
17	2300.00	L	Cross-Site Scripting without input Validation (cross-site-scripting)	Webapp Security	Cross Site Scripting	exploit cow-bell shop guest book (stored xss)
18	2300.00	L	Cross-Site Scripting with client-side input validation	Webapp Security	Cross Site Scripting	exploit cow-bell shop guest book (stored xss with input val)
19	2301.00	L	Second Order XSS over Web Services (GlockenFranz)	Webapp Security	Cross Site Scripting	exploit cow-bell shop via second app (glocken franz, second order)
20	2303.00	L	Internet Explorer Vulnerability (Image Tag Vulnerability)	Client Security Windows	Find Vulnerability	how to find zero-day exploits in browsers (fuzzing lab)
21	2303.00	L	Malware Distribution through Cross-Site Scripting (Firelinking)	Malware Windows	Malware Delivery	exploit firefox zero-day exploit (requires firefox 1.x)
22	2310.00	L	SQL Injection on Logon Page	Webapp Security	SQL Injection	exploit sql injection and bypass authentication (blind sql injectin)
23	2310.00	L	SQL Injection with UNION	Webapp Security	SQL Injection	exploit sql injection and disclose name, creditcard, users from table
24	2320.00	L	Session Stealing - URL Redirect	Webapp Security	URL Redirection	exploit trust relationship -redirect to landing page after authentication
25	2330.00	L	Java Object Inspector (Extended)	Webapp Security	Authorization Attack	exploit business logic in client apps (difficult to change something)
26	2330.00	L	Java Object Inspector (Prepared)	Webapp Security	Authorization Attack	exploit business logic in client apps (difficult to change something)
27	2501.00	L	Reverse Proxy Attack	Webapp Security	Entry Server	place a web application firewall in front of our vuln web app part 1
28	2501.00	L	Reverse Proxy Attack + MOD_REPLACE	Webapp Security	Phishing	place a web application firewall in front of our vuln web app part 2
29	2502.00	L	Abuse of E-Mail Forms	Webapp Security	Spam	MailForm Injection
30	2600.00	L	XML Injection	Webapp Security	XML Security	exploit xml generator and gather more than considered by the app
31	2600.00	L	XML Port Scan	Webapp Security	XML Security	find valid open ports through xml injection
32	2600.00	L	XML URL Enumeration	Webapp Security	XML Security	find valid url names through xml injection
33	2600.00	L	XML Path Traversal	Webapp Security	XML Security	find valid directories and files on the server through xml injection

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
34	2601.00	L	Web Service Enumeration (WSDL)	Webapp Security	WSDL	find valid credit cards through hidden wsdl links
35	2605.00	L	XPath Injection (SQL for XML Attack)	Webapp Security	XML Security	exploit xpath vulnerability and list all transactions
36	2650.00	L	RSS + XSS mit JavaScript, das die Session verschickt.	Webapp Security	Cross Site Scripting	exploit xss through rss feed (second order)
37	2651.00	L	XSRF (Request Forgery)	Webapp Security	Session Attacks	exploit xsrf for the cow-bell shop. Buy bells behind the scene
38	2652.00	L	Web 2.0 Worm Development	Webapp Security	Web 2.0	develop a java script worm for the Hacking-Lab social software
39	2653.00	L	Java DWR Migration mit Mailform (aka Ajax Migration in Hacklab)	Webapp Security	Web 2.0	migrate web 1.0 app into a web 2.0 app with DWR and eclipse
40	2654.00	L	ActiveX Exploitation (HP DLL)	Client Security Windows	Client Exploitation	exploit activex vulnerability and run system commands
41	2655.00	L	Flash Exploitation (csPreload)	Client Security Windows	Client Exploitation	exploit flash app and start xss attack
42	2656.00	L	Crypto Analysis Isrunase.exe	Reverse Engineering	Crypto	exploit weak encryption algorithm in Isrunase.exe
43	2657.00	L	BHO Lab	Webapp Security	Client Security	exploit browser helper object to gain Internet Explorer controls
44	2658.00	L	Web 2.0 Intro Lab	Webapp Security	Web 2.0	Intro lab for web 2.0 (play with firebug and tools)
45	2663.00	L	JavaScript Malware Analysis	Malware Web	Java Script	explain java script malware
46	2664.00	L	JSON Hijacking	Webapp Security	JSON Hijacking	Create JSON hijacking page for cow bell shop (credit card in profile, aka
47	2665.00	L	XSS Camtasia Movie	Webapp Security	Flash	Exploit Camtasia Flash XSS
48	2700.00	L	Application Logging	Webapp Security	Forensic Analysis	perform a web forensic analysis - explain what is happened
49	3001.00	L	Vulnerability Scanning	Network Security	Scanning	Perform a nessus scan against the Hacking-Lab infrastructure
50	3001.00	L	Discovery and Fingerprinting	Network Security	Fingerprinting	fingerprint the services in Hacking-Lab
51	3002.00	L	Netzwerk und Domänensuche	Network Security	Information	find out more about a target network with information gathering technique
52	3002.00	L	Google Web Research	Network Security	Information	find out more about a target network with information gathering technique
53	3002.00	L	DNS Analyse	Network Security	DNS Analysis	find out more about a target network with dns queries
54	3002.00	L	Enumeration und Banner Grabbing	Network Security	Information	find out more about products with netcat (netcat intro lab)
55	3003.00	L	Online Cracking Attack of Windows NT 4.0 Server	Windows Security	Cracking	online cracking against nt4 server
56	3003.00	L	Online Cracking Attack of W2K Domain Controller	Windows Security	Cracking	online cracking against windows 2000 server
57	3003.00	L	Offline Cracking Attacks	Windows Security	Cracking	offline cracking dictionary and brute force attack
58	3003.00	L	Offline Cracking Attacks Active Directory	Windows Security	Cracking	offline cracking dictionary and brute force attack
59	3003.00	L	Online Cracking Attack	Windows Security	Cracking	offline cracking dictionary and brute force attack
60	3005.00	L	Direct Attack SUN Solaris	Unix Security	Buffer Overflow	exploit telnet vulnerability in solaris 7
61	3005.00	L	Buffer Overflow DCOM RPC	Windows Security	Buffer Overflow	remote exploit dcom rpc vulnerability
62	3005.00	L	Buffer Overflow W2K LPD (Inside-Out)	Windows Security	Buffer Overflow	exploit windows2000 lpd vulnerability
63	3006.00	L	Exploiting with Metasploit Framework	Hacker Tools	MetaSploit	intro lab for metasploit

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
64	3008.00	L	ARP-Spoofing & DNS Spoofing	Network Security	Pharming	perform arp spoofing + dns spoofing
65	3008.00	L	ARP-Spoofing und Snooping	Network Security	Pharming	perform arp spoofing + network interception
66	3009.00	L	Bypass Anti-Virus	Malware Windows	Bypass Anti-Virus	bypass anti-virus pattern lab
67	3009.00	L	Merging of EXE	Malware Windows	Obfuscation	merge trojan and useful tool with script tool
68	3010.00	L	DNS Tunnel	Tunneling	DNS Tunnel	exploit dns tunneling attack
69	3010.00	L	Inside-Out mit HTTP Tunnel	Tunneling	Tunneling	exploit http tunneling attack with htc/hts
70	3012.00	L	Spyware	Observation	Spytech	play with a commercial surveillance software (spytech)
71	3014.00	L	Wireshark Extended Features	Sniffing		learn more about wireshark
72	3016.00	L	Static vs. Dynamic Binary Inspection	Malware Windows	Malware Analysis	windows binary analysis (Foong server.exe and exploit.hex)
73	3018.00	L	HTML Mail (SMB Attack)	Windows Security	HTML Link	windows smb relaying attack
74	3018.00	L	IPC\$NULL SESSION Username Enumeration	Windows Security	IPC\$ Null Session	exploit windows IPC\$Null session
75	3018.00	L	SMB Relay (Angriff auf Client-PC)	Windows Security	SMB Relay	exploit smb relaying attack with Metasploit
76	3019.00	L	Inside-Out mit Netcat	Tunneling	Tunneling	Inside-out attack with netcat
77	3020.00	L	Snooping HTTP BasicAuth	Network Security	Sniffing	Exploit http basic auth - man in the middle
78	3020.00	L	Sniffen von TCP/IP 3-Way-Handshakes + Telnet Passworten	Network Security	Sniffing TCP/IP Han	wireshark tcp/ip intro lab
79	3022.00	L	vlan trunk attack	Network Security	Packet Forgery	exploit vlan trunk attack
80	3022.00	L	vlan double encapsulation	Network Security	Packet Forgery	exploit vlan double encapsulation attack
81	3023.00	L	portsecurity	Network Security	Portsecurity	exploit mac based port security
82	3023.00	L	portsecurity hub attack	Network Security	Portsecurity HUB	exploit mac based port security
83	3024.00	L	Breakout rbash	Unix Security	App Breakout	exploit restricted shell (rbash breakout)
84	3024.00	L	Gain Root	Unix Security	Privilege Escalation	gain root privileges on the target linux machine
85	3027.00	L	Microsoft RPC Traffic Analyse	Sniffing	mitm	wireshark lab for the rdp protocol
86	3028.00	L	Other Network Capturing Tools	Sniffing	mitm	intro lab for network forensic lab
87	3029.00	L	Network Forensic Challenge	Forensic Network	mitm	intro lab for network forensic lab
88	3030.00	L	SSH Protocol Lab	Network Security	mitm	intro lab for ssh
89	3031.00	L	SSL/TLS Protocol Lab	Network Security	mitm	intro lab for ssl/tls
90	3032.00	L	Analyse Kerberos Protocol	Network Security	mitm	intro lab for kerberos
91	4002.00	L	VPN Infomration Gathering and Aggressive Mode Hacking	Network Security	IKE Scanning	find and exploit IKE based VPN
92	4003.00	L	WEP Key Cracking (Extended)	Wireless Security	WEP Cracking	find web key (web cracking)
93	4003.00	L	WEP Key Cracking (Prepared)	Wireless Security	WEP Cracking	find web key (web cracking)

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
94	4005.00	L	USB Insecurity - USB Switchblade	Malware Windows	USB Switchblade	Analyse processes, OllyDdg
95	4010.00	L	Sony Rootkit	Malware Windows	Malware Analysis	exploit sony rootkit - explore the malware
96	4010.00	L	Sony Rootkit - Visualization with Planet Sony	Malware Windows	Malware Analysis	exploit sony rootkit - explore the malware
97	4011.00	L	Demonstrate how Skype and the Skype API can be used as a inside-out	Malware Windows	Skype	intro lab skype
98	4020.00	L	Fuzzing Internet Explorer	Client Security Windows	Find Vulnerability	find new vulnerabilities with fuzzing
99	4021.00	L	Identifying content type using MIME Sniffing	Forensic Windows	Malware Analysis	bypass content filter
100	4021.00	L	Transfer encoding in HTML meta data and effects in browser	Webapp Security	Encodings	explore the meta data types
101	4030.00	L	The virus scanner comparison test	Malware Infection	Malware Analysis	intro lab with virus total
102	4032.10	L	Web Content Filter	Forensic Windows	Malware Analysis	File Type Identification
103	4032.20	L	Malware Analysis in Sandbox	Forensic Sandbox	Malware Analysis	Threat Report (Sandbox)
104	4032.30	L	Content-Filter - Web-Content-Filter - EXE / BLA	Malware Infection	Bypass Content	Dansguardian Suffix Block
105	4032.31	L	Content-Filter - Web-Content-Filter - EXE / BLA	Malware Infection	Bypass Content	Dansguardian Pattern Block
106	4032.40	L	Bypass Content Filter using SSL	Malware Infection	Bypass Content	Dansguardian Bypass Block with SSL
107	4032.50	L	Bypass Content Filter using SSL	Malware Infection	Bypass Content	Dansguardian SSL Bridge Block
108	4032.60	L	Bypass Content Filter using SSL	Malware Infection	Bypass Content	Dansguardian Final Bypass
109	4033.10	L	Anonymizer	Tunneling	Hiding Technique	MegaProxy
110	4033.20	L	TOR	Tunneling	Tor	explore the Tor Anonymizer Network
111	4034.10	L	Tunneling POP3 via SSH	Tunneling	Tunneling	exploit tunnel: Tunneling POP3 via SSH
112	4034.20	L	Tunneling POP3 via SSH wird verhindert	Tunneling	Tunneling	exploit tunnel: Tunneling POP3 via SSH wird verhindert
113	4036.00	L	Terminal Server Surfing	SBC	Client Security	showcase: Internet Explorer on terminal server
114	4040.00	L	Anziehen von Client-Laufwerken	SBC	Malware Delivery	exploit client mappings in rdp protocol
115	4041.00	L	Abort execution of Login-Scripts	SBC	App Breakout	exploit terminal server logon scripts
116	4041.00	L	Installation of a backdoor über through logon scripts.	SBC	Privilege Escalation	Gain Admin Privs using printer driver
117	4042.00	L	Terminal Server Ausbrechen aus Applikationen	SBC	App Breakout	gain a full desktop from a reduced terminal server session (outlook
118	4043.00	L	Backend proxy used as media for infiltrating code and exfiltrating data.	SBC	Data Theft	offline cracking sam from rdp session
119	4044.00	L	RDP connection used as media for infiltrating code and exfiltrating data.	SBC	Data Theft	visual data transfer with QR Code
120	5003.00	L	MS Word Fast Save	Forensic Windows	File Analysis	forensic: intro to MS Office 2000 fast save feature
121	5003.00	L	MS Word Meta Data	Forensic Windows	File Analysis	forensic: intro to ms word 2000 meta data
122	5003.00	L	MS Word Temp Files	Forensic Windows	File Analysis	forensic: intro to ms office 2000 temp files generation
123	5003.00	L	MS Word Track Changes	Forensic Windows	File Analysis	forensic: intro to ms office 2000 track change features

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
124	5003.00	L	Uncover PDF	Forensic Windows	File Analysis	forensic: uncover hidden data from pdf
125	5004.00	L	File Analysis	Forensic Windows	Malware Analysis	forensic: uncover packed trojan
126	5005.00	L	Slackspace	Forensic Linux	Forensic Analysis	forensic: uncover slackspace data
127	5005.00	L	ADS	Forensic Windows	Hiding Technique	forensic: uncover ADS (alternative data streams)
128	5005.00	L	Steganography	Forensic Windows	Hiding Technique	forensic: intro to steganography
129	5007.00	L	Sleuthkit Analysis	Forensic Windows	Forensic Analysis	Intro to forensic tools: Sleuthkit/Autopsy
130	5008.00	L	Search for illegal pictures	Forensic Windows	Evidence	forensic: search for illegal pictures
131	5009.00	L	Analyze Linux Live System	Forensic Linux	Rootkit	forensic: analyze live system (linux)
132	5013.00	L	Tcpdump Analysis and Backdoor traffic analysis	Intrusion Detection	Snort	forensic: analyze tcpdump file (trojan traffic)
133	5014.00	L	Spyware identification	Forensic Windows	Malware	forensic: identification of malware
134	5014.00	L	Eicar within PDF	Forensic Windows	Malware Analysis	forensic: Eicar in PDF
135	5015.00	L	Analyse apache, fw, mysql log	Forensic Webapp	Correlation	forensic: analyze web app logs - find the attacker
136	5017.00	L	Sparc Solaris 7 Sendmail Rootkit	Unix Security	Malware	forensic: Rootkit Detection in sendmail package
137	5018.00	L	Malicious Word mit Makro für das Versenden von Cookies	Malware	Malware	forensic: uncover malware makros in office file
138	5019.00	L	FastCrack	Windows Security	Reset login	windows reset login account
139	5020.00	L	PW geschütztes ZIP	Reverse Engineering	Information	uncover content of password protected zip file
140	5021.00	L	PW geschütztes Excel	Reverse Engineering	Information	uncover content of password protected excel file
141	5022.00	L	NFS Portmapper Bypass	Network Security	bypass acl	exploit ACL and mount an NFS share
142	5023.00	L	Hash Injection	Windows Security	bypass password	gain domain admin privileges (microsoft)
143	5024.00	L	LockPicking Exercise	Lock Picking	bypass locks	
144	5025.00	L	SSL Web Attack	Webapp Security	bypass ssl/tls	gain access to ssl protected page
145	5026.00	L	MySQL Breakin	Database Security	bypass sql protection	gain access to mysql data
146	5027.00	L	Easter Egg with QR Code	Easter Egg	easter egg	swiss cyber storm II easter egg (not a wargame)
147	5028.00	L	Conficker Exploit	Windows Security	remote exploit	exploit conficker vulnerability
148	5029.00	L	Oracle Attack	Database Security	web exploit	exploit oracle web vulnerabilities
149	5030.00	L	Cross Site Scripting	Webapp Security	web exploit	exploit cow bell show xss vulnerabilities
150	5031.00	L	Cross Site Request Forgery, xsrf	Webapp Security	web exploit	exploit xsrf vulnerability in cow-bell shop
151	5032.00	L	URL Redirection Attack	Webapp Security	web exploit	exploit url redirection attack to malicious login page
152	5033.00	L	Click Jacking	Webapp Security	web exploit	exploit click jacking vulnerability
153	5034.00	L	WLAN Karma Attack	Network Security	mitm	perform wlan karma attack

	A	B	C	D	E	F
1	Compass Course Modules					
2	Sprache: EN					
3						
4	Modul Number	Typ	Name	Chapter	Attack Type	Details
154	5035.00	L	Oracle Hacking Alexander Kornbrust	Database Security	web exploit	more stuff with oracle hacking
155	5036.00	L	Hacking Secure Browser	Client Security Windows	client exploit	exploit prism browser
156	5037.00	L	Privilege Escalation, Challenge of the Month	Windows Security	client exploit	gain local admin privileges
157	3001.00	L	Advanced Nmap auf Conficker VM bei ASL Master	Penetration Testing	fingerprinting	find out vulnerable conficker hosts (conficker identification)
158	5039.00	L	Nessus mit nasl	Penetration Testing	fingerprinting	perform nessus scan with NASL interface
159	3010.00	L	Inside-Out elab Infrastructure	Network Security	remote control	perform inside-out channel
160	5043.00	L	VOIP Snom Phone Authentication ByPass	Network Security	bypass acl	exploit voip snom vulnerability
161	5044.00	L	SSL Renegotiation Attack	Network Security	bypass ssl/tls	understand ssl renegotiation vulnerability
162	5046.00	L	Hacking Prism Browser	Client Security Windows	client exploit	wargame for hacking prism browsers
163	5047.00	L	Forensic Wargame Christiaan Beek from ITU	Forensic Windows	information gathering	explain the warsaw gang scene
164	6001.00	L	Hardening Apache (File Permissions)	Unix Security	Hardening	Apache File Permissions
165	6001.00	L	Hardening Apache CHROOT	Unix Security	Hardening	Chroot
166	7000.00	L	LiveHttpHeader	Malware	Observation	Observation Firefox Plugin
167	7001.00	L	Encrypted File System (EFS)	Client Security Windows	Crypto	EFS file disclosure
168	7002.00	L	GOT ROOT	Unix Security	Privilege Escalation	Got Root
169	7003.00	L	Terminal Server Hacking	SBC	Data Theft	Data steeling
170	7004.00	L	Restricted Shell Breakout	Unix Security	Privilege Escalation	rbash exploit
171	7005.00	L	Shatter Attack	Client Security Windows	Privilege Escalation	Gain local Admin privs
172	7006.00	L	Windows Backdoor Execution	Malware Infection	Malware Analysis	Malware Execution
173	7007.00	L	Bypass Antivirus Checks	Malware Infection	Bypass Anti-Virus	Modify nc.exe
174	7008.00	L	Reverse Proxy + mod_security 2	Webapp Security	Intrusion Detection	mod_security
175	7009.00	L	XML Attack + Password Cracking	Webapp Security	Cracking	Password cracking
176	7010.00	L	DNS Host Name Change	Network Security	Pharming	DNS host name change
177	7011.00	L	Tcpdump Analysis and snort rule for dns tunneling	Intrusion Detection	Intrusion Detection	Snort rule development
178	7013.00	L	Java Applet Hacking	Webapp Security	Authorization Bypass	Applet Hacking
179	7014.00	L	SIP Attack	Network Security	Packet Forgery	SIP signaling service
180	8008.00	L	Buffer Overflow Exploiting Server.exe auf csl-ts.compa.ny	Reverse Engineering	reverse engineer	