0	PT1-003 Objective	Details
1	Engagement Management	
3	Summarize pre-engagement activities.	
4		Scope definition
5		Regulations, frameworks, and standards
6		Privacy regulations
7		Security regulations
8		Rules of engagement
9		(Scope) exclusions
10		Test cases
11		Escalation proces
12		Testing window
13		Agreement types
14		Non-disclosure agreement (NDA)
15		Master service agreement (MSA
16		Statement of work (SoW)
17		Terms of service (ToS)
18		Target selection
19		Classless Inter-Domain Routing (CIDR) ranges
20		Domains
21		Internet Protocol (IP) addresses
22		Uniform Resource Locator (URL)
23		Assessment types
24		Web assessment
25		Network assessment
26		Mobile assessment
27		Cloud assessment
28		Application programming interface (API) assessment
29		Application assessment
30		Wireless assessment
31		Shared responsibility model
32		Hosting provider responsibilities
33		Customer responsibilities
34		Penetration tester responsibilities
35		Third-party responsibilities
36		Legal and ethical considerations
37		Authorization letters
38		Mandatory reporting requirements
39		Risk to the penetration tester
41	Explain collaboration and communication activities.	
42		Peer review
43		Stakeholder alignment
44		Root cause analysis
45		Escalation path
46		Secure distribution
47		Articulation of risk, severity, and impact
48		Goal reprioritization
49		Business impact analysis
50		Client acceptance
52	Compare and contrast testing frameworks and methodologies.	

53		Open Source Security Testing Methodology Manual (OSSTMM)
54		Council of Registered Ethical Security Testers (CREST)
55		Penetration Testing Execution Standard (PTES)
56		MITRE ATT&CK
57		Open Web Application Security Project (OWASP) Top 10
58		OWASP Mobile Application SecurityVerification Standard (MASVS)
59		Purdue model
60		Threat modeling frameworks
61		DREAD
62		STRIDE
63		OCTAVE
65	Explain the components of a penetration test report.	
66		Report Format alignment
67		Documentation specifications
68		Risk scoring
69		Definitions of terms
70		Report components
71		Executive summary
72		Methodology
73		Detailed findings
74		Attack narrative
75		Recommendations
76		Remediation guidance
77		Test limitations and assumptions
78		Reporting considerations
79		Legal considerations
80		Ethical considerations
81		Quality control (QC)
82		Artificial intelligence (AI) considerations
84	Given a scenario, analyze the findings and recommend the appropriate remediation within a report	
85		Technical controls
86		System hardening
87		Sanitize user input/parameterize queries
88		Multifactor authentication
89		Encryption
90		Process-level remediation
91		Patch management
92		Key rotation
93		Certificate management
94		Secrets management solution
95		Network segmentation
96		Infrastructure security controls
97		Administrative controls
98		Role-based access control
99		Secure software developmentlife cycle
100		Minimum password requirements
101		Policies and procedures
102		Physical controls
103		Access control vestibule
104		Biometric controls

105		Videsurveillance
106		Operational controls
107		Job rotation
108		Time-of-day restrictions
109		Mandatory vacations
110		User training
113	Reconnaissance and Enumeration	
115	Given a scenario, apply information gathering techniques.	
116		Active and passive reconnaissance
117		Open-source intelligence (OSINT)
118		Social media
119		Job boards
120		Scan code repositories
121		Domain Name System (DNS)
122		DNS lookups
123		Reverse DNS lookups
124		Cached pages
125		Cryptographic flaws
126		Password dumps
127		Network reconnaissance
128		Protocol scanning
129		TCP / UDP
130		Certificate transparency logs
131		Information disclosure
132		Search engine analysis/ enumeration
133		Network sniffing
134		Internet of Things (IoT) and operational technology (OT) protocols
135		Banner grabbing
136		Hypertext Markup Language (HTML) scraping
138	Given a scenario, apply enumeration techniques.	
139		Operating system (OS) fingerprinting
140		Service discovery
141		Protocol enumeration
142		DNS enumeration
143		Directory enumeration
144		Host discovery
145		Share enumeration
146		Local user enumeration
147		Email account enumeration
148		Wireless enumeration
149		Permission enumeration
150		Secrets enumeration
151		Cloud access keys
152		Passwords
153		API keys
154		Session tokens
155		Attack path mapping
156		Web application firewall (WAF) enumeration
157		Origin address
158		Web crawling

159		Manual enumeration
160		Robots.txt
161		Sitemap
162		Platform plugins
164	Given a scenario, modify scripts for reconnaissance and enumeration.	
165		Information gathering
166		Data manipulation
167		Scripting languages
168		Bash
169		Python
170		PowerShell
171		Logic constructs
172		Loops
173		Conditionals
174		Boolean operator
175		String operator
176		Arithmetic operator
177		Use of libraries, functions, and classes
179	Given a scenario, use the appropriate tools for reconnaissance and enumeration	
180		Wayback Machine
181		Maltego
182		Recon-ng
183		Shodan
184		SpiderFoot
185		WHOIS
186		nslookup/dig
187		Censys.io
188		Hunter.io
189		DNSdumpster
190		Amass
191		Nmap
192		Nmap Scripting Engine (NSE)
193		theHarvester
194		WiGLE.net
195		InSSIDer
196		OSINTframework.com
197		Wireshark/tcpdump
198		Aircrack-ng
200	Vulnerability Discovery and Analysis	
202	Given a scenario, conduct vulnerability discovery using various techniques.	
203		Types of vulnerability scans
204		Container scans
205		Container Sidecar scans
206		Application scans
207		Dynamic application security testing (DAST)
208		Interactive application security testing (IAST)
209		Software composition analysis (SCA)
210		Static application security testing (SAST)
211		Infrastructure as Code (IaC)
212		Source code analysis

213		Mobile scan
214		Mobile Network scans
215		TCP/UDP scan
216		Stealth scans
217		Host-based scans
218		Authenticated vs. unauthenticated scans
219		Secrets scanning
220		Wireless
221		Service set identifier (SSID) scanning
222		Channel scanning
223		Signal strength scanning
224		Industrial control systems (ICS) vulnerability assessment
225		Manual assessment
226		Port mirroring Tools
227		Vulnerability discovery tools
228		BloodHound
229		Tenable Nessus
230		PowerSploit
231		Grype
232		Trivy
233		Kube-hunter
234		Nikto
235		Greenbone/Open Vulnerability Assessment Scanner (OpenVAS)
236		TruffleHog
238	Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases	
239		Validate scan, reconnaissance, and enumeration results
240		False positives
241		False negatives
242		True positives
243		Scan completeness
244		Troubleshooting scan configurations
245		Public exploit selection
246		Use scripting to validate results
249	Explain physical security concepts.	
250		Tailgating
251		Universal Serial Bus (USB) drops
252		Site surveys
253		Badge cloning
254		Lock picking
257	Attacks and Exploits	
259	Given a scenario, analyze output to prioritize and prepare attacks.	
260		Target prioritization
261		High-value asset identification
262		Target Descriptors and metrics
263		Common Vulnerability Scoring System (CVSS) base score
264		Common Vulnerabilities and Exposures (CVE)
265		Common Weakness Enumeration (CWE)
266		Exploit Prediction Scoring System (EPSS)
267		End-of-life software/systems
268		Default configurations

269		Running services
270		Vulnerable encryption methods
271		Defensive capabilities
272		Capability selection
273		Attack preparation Tool selection
274		Attack preparation Exploit selection and customization
275		Attack preparation Code analysis
276		Attack preparation Documentation
277		Attack preparation Attack path
278		Attack preparation Low-level diagram creation
279		Attack preparation Storyboard
280		Attack preparation Dependencies
281		Consideration of scope limitations Labeling sensitive systems
284	Given a scenario, perform network attacks using the appropriate tools.	
286		Default credentials
287		On-path attack
288		Certificate services
289		Misconfigured services exploitation
290		Virtual local area network(VLAN) hopping
291		Multihomed hosts
292		Relay attack
293		Share enumeration
294		Packet crafting
296		NSE
297		Metasploit
298		Netcat
299		Nmap
300		Impacket
301		CrackMapExec (CME)
302		Wireshark/tcpdump
303		msfvenom
304		Responder
305		Hydra
309	Given a scenario, perform authentication attacks using the appropriate tools.	
311		Multifactor authentication (MFA) fatigue
312		Pass-the-hash attacks
313		Pass-the-ticket attacks
314		Pass-the-token attacks
315		Kerberos attacks
316		Lightweight Directory Access Protocol (LDAP) injection
317		Dictionary attacks
318		Brute-force attacks
319		Mask attacks
320		Password spraying
321		Credential stuffing
322		OpenID Connect (OIDC) attacks
323		Security Assertion Markup Language (SAML) attacks
325		CME
326		Responder
327		hashcat

328		John the RipperHydra
329		BloodHound
330		Medusa
331		Burp Suite
334	Given a scenario, perform host-based attacks using the appropriate tools.	
336		Privilege escalation
337		Credential dumping
338		Circumventing security tools
339		Misconfigured endpoints
340		Payload obfuscation
341		User-controlled access bypass
342		Shell escape
343		Kiosk escape
344		Library injection
345		Process hollowing and injection
346		Log tampering
347		Unquoted service path injection
349		Mimikatz
349		Rubeus
350		Certify
351		Seatbelt
352		PowerShell/PowerShell Integrated Scripting Environment (ISE)
353		PsExec
354		Evil-WinRM
355		Living off the land binaries (LOLbins)
357	Given a scenario, perform web application attacks using the appropriate tools	
359		Brute-force attack
360		Collision attack
361		Directory traversal
362		Server-side request forgery (SSRF)
363		Cross-site request forgery (CSRF)
364		Deserialization attack
365		Injection attacks
366		Structured Query Language (SQL) injection
367		Command injection
368		Cross-site scripting (XSS)
369		Server-side template injection
370		Insecure direct object reference
371		Session hijacking
372		Arbitrary code execution
373		File inclusions
374		Remote file inclusion (RFI)
375		Local file inclusion (LFI)
376		Web shell
377		API abuse
378		JSON Web Token (JWT) manipulation
380		Truffle
380		Burp Suite
381		Zed Attack Proxy (ZAP)
382		Postman

383		sqlmap
384		Gobuster/DirBuster
385		Wfuzz
386		WPScan
388	Given a scenario, perform cloud-based attacks using the appropriate tools.	
390		Metadata service attacks
391		Identity and access management misconfigurations
392		Third-party integrations
393		Resource misconfiguration
394		Network segmentation
395		Network controls
396		Identity and access management (IAM) credentials
397		Exposed storage buckets
398		Public access to services
399		Logging information exposure
400		Image and artifact tampering
401		Supply chain attacks
402		Workload runtime attacks
403		Container escape
404		Trust relationship abuse
406		Pacu
407		Docker Bench
408		Kube-hunter
409		Prowler
410		ScoutSuite
411		Cloud-native vendor tools
414	Given a scenario, perform wireless attacks using the appropriate tools.	
416		Wardriving
417		Evil twin attack
418		Signal jamming
419		Protocol fuzzing
420		Packet crafting
421		Deauthentication
422		Captive portal
423		Wi-Fi Protected Setup (WPS) personal identification number (PIN) attack
425		WPAD
426		WiFi-Pumpkin
427		Aircrack-ng
428		WiGLE.net
429		InSSIDer
430		Kismet
432	Given a scenario, perform social engineering attacks using the appropriate tools	
434		Phishing
435		Vishing
436		Whaling
437		Spearphishing
438		Smishing
439		Shoulder surfing
440		Tailgating
441		Eavesdropping

442		Watering hole
443		Impersonation
444		Credential harvesting
445		Dumpster diving
446		Surveillance
449		Gophish
450		Evilginx
451		theHarvester
452		Maltego
453		Recon-ng
454		Browser Exploitation Framework (BeEF)
455		Social Engineering Toolkit (SET)
457	Explain common attacks against specialized systems.	
459		Mobile attacks
460		Information disclosure
461		Jailbreak/rooting
462		Permission abuse
463		AI attacks
464		Prompt injection
465		Model manipulation
466		OT
467		Register manipulation
468		CAN bus attack
469		Modbus attack
470		Plaintext attack
471		Replay attack
472		Near-field communication (NFC)
473		Bluejacking
474		Radio-frequency identification (RFID)
475		Bluetooth spamming
478		tcprelay
479		Wireshark/tcpdump
480		MobSF
481		Frida
482		Drozer
483		Android Debug Bridge (ADB)
484		Bluecrack
485		Scapy
488	Given a scenario, use scripting tautomate attacks.	
489		PowerShell
490		Empire/PowerSploit
491		PowerView
492		PowerUpSQL
493		AD search
494		Bash
495		Input/output management
496		Data manipulation
497		Python
498		Impacket
499		scapy

500		Breach and attack simulation (BAS)
501		Caldera
502		Infection Monkey
503		Atomic Red Team
506	Post-exploitation and Lateral Movement	
508	Given a scenario, perform tasks testablish and maintain persistence.	
509		Scheduled tasks/cron jobs
510		Service creation
511		Reverse shell
512		Bind shell
513		Add new accounts
514		Obtain valid account credentials
515		Registry keys
516		Command and control (C2) frameworks
517		Backdoor
518		Web shell
519		Trojan
520		Rootkit
521		Browser extensions
522		Tampering security controls
524	Given a scenario, perform tasks tmove laterally throughout the environment.	
525		Pivoting
526		Relay creation
527		Enumeration
528		Service discovery
529		Network traffic discovery
530		Additional credential capture
531		Credential dumping
532		String searches
533		Service discovery
534		Server Message Block (SMB)/ fileshares
535		Remote Desktop Protocol (RDP)/ Virtual Network Computing (VNC)
536		Secure Shell (SSH)
537		Cleartext
538		LDAP
539		Remote Procedure Call (RPC)
540		File Transfer Protocol (FTP)
541		Telnet
542		Hypertext Transfer Protocol (HTTP)/ Hypertext Transfer Protocol Secure (HTTPS)
543		Web interfaces
544		Line Printer Daemon (LPD)
545		JetDirect
546		RPC/Distributed Component Object Model (DCOM)
547		Process IDs
548		Window Management Instrumentation (WMI)
549		Window Remote Management (WinRM) Tools
550		LOLBins
551		mmc.exe
552		rundll
553		msbuild

554		route
555		strings/findstr.exe
556		Netstat
557		Net commands
558		cmd.exe
559		explore.exe
560		ftp.exe
561		Covenant
562		CrackMapExec
563		Impacket
564		Netcat
565		sshuttle
566		Proxychains
567		PowerShell ISE
568		Batch files
569		Metasploit
570		PsExec
571		Mimikatz
574	Summarize concepts related to staging and exfiltration.	
575		File encryption and compression
576		Covert channel
577		Steganography
578		DNS exfil
579		Internet Control Message Protocol (ICMP) exfil
580		HTTPS exfil
581		Email exfil
582		Cross-account resources exfil
583		Cloud storage exfil
584		Alternate data streams exfil
585		Text storage sites exfil
586		Virtual drive mounting exfil
588	Explain cleanup and restoration activities.	
590		Remove persistence mechanisms
591		Revert configuration changes
592		Remove tester-created credentials
593		Remove tools
594		Spin down infrastructure
595		Preserve artifacts
596		Secure data destruction
597		Payment Card Industry Data Security Standard (PCI DSS)
598		General Data Protection Regulation (GDPR)
599		Country limitations
600		Local laws
601		Local government requirements
602		National Institute of Standards and Technology (NIST)
603		Information Systems Security Assessment Framework (ISSAF)
604		Validate scope of engagement
605		Question the client/review contracts
606		Background checks of penetration testing team
607		Identify criminal activity

608		Immediately report breaches/criminal activity
609		load balancer detection
610		firewall detection
611		antivirus detection
612		Considerations of vulnerability scanning
613		bandwidth limitations
614		fragile systems
615		Stress testing for availability
616		Exploit DB
617		Packet Storm
618		ARP poisoning
619		exploit chaining
620		NAC network access control bypass
621		MAC media access control bypass
622		Link-Local Multicast Name Resolution (LLMNR)/NetBIOS-Name Service (NBT-NS) poisoning
623		New Technology LAN Manager (NTLM) relay attacks
624		business logic flaws
625		race conditions
626		lack of error handling
627		lack of code signing
628		insecure data transmission
629		session fixation
630		REST
631		SOAP
632		Extensible Markup Language-Remote Procedure Call (XML-RPC)
633		resource exhaustion
634		cloud malware injection attacks
635		denial of service attacks
636		side-channel attacks
637		direct-to-origin attacks
638		software development kit
639		reverse engineering
640		sandbox analysis
641		spamming
642		insecure mobile storage
643		mobile passcode vulnerabilities
644		certificate pinning
645		dependency vulnerabilities
646		patching fragmentation
647		execution of activities using root
648		over-reach of mobile permissions
649		biometrics integrations
650		business logic flaws
651		needle
652		ettercap
653		APK Studio
654		APKX
655		BLE attacks
656		Special considerations in IoT attacks
657		Cleartext

658		Intelligent platform management interface (IPMI)
659		Vulnerabilities related to supervisory control and data acquisition (SCADA)/ Industrial Internet of Things (IIoT)/ industrial control system
660		VM escape
661		Hypervisor vulnerabilities
662		VM repository vulnerabilities
663		Pretext for an approach
664		Methods of influence
665		Authority
666		Scarcity
667		Social proof
668		Likeness
669		Fear
670		Urgency
671		Report audience
672		Note taking
673		primary contact
674		technical contact
675		follow-up actions / retest
676		data destruction process
677		
678		
679		
680		
681		
682		
683		
684		
685		
686		
687		
688		
689		
690		
691		
692		
693		
694		
695		
696		
697		
698		
699		
700		
701		
702		
703		
704		
705		
706		
707		

708		
709		
710		
711		
712		
713		
714		
715		
716		
717		
718		
719		
720		
721		
722		
723		
724		
725		
726		
727		
728		
729		
730		
731		
732		
733		
734		
735		
736		
737		
738		
739		
740		
741		
742		
743		
744		
745		
746		
747		
748		
749		
750		
751		
752		
753		
754		
755		
756		
757		

758		
759		
760		
761		
762		
763		
764		
765		
766		
767		
768		
769		
770		
771		
772		
773		
774		
775		
776		
777		
778		
779		
780		
781		
782		
783		
784		
785		
786		
787		
788		
789		
790		
791		
792		
793		
794		
795		
796		
797		
798		
799		
800		
801		
802		
803		
804		
805		
806		
807		

808		
809		
810		
811		
812		
813		
814		
815		
816		
817		
818		
819		
820		
821		
822		
823		
824		
825		
826		
827		
828		
829		
830		
831		
832		
833		
834		
835		
836		
837		
838		
839		
840		
841		
842		
843		
844		
845		
846		
847		
848		
849		
850		
851		
852		
853		
854		
855		
856		
857		

PT1-003	PT0-002
1.0	
1.1	
1.1	1.2
1.1	1.1
1.1	1.1
1.1	1.1
1.1	1.2
1.1	1.2
1.1	1.2
1.1	4.3
1.1	1.2
1.1	1.1
1.1	1.1
1.1	1.1
1.1	1.1
1.1	1.2
1.1	1.2
1.1	1.2
1.1	1.2
1.1	1.2
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	x
1.1	1.3
1.1	x
1.1	x
1.1	1.1
1.1	1.1
1.1	1.3
1.1	1.3
1.2	
1.2	x
1.2	4.1
1.2	x
1.2	4.3
1.2	4.1
1.2	4.1
1.2	4.3
1.2	4.1
1.2	4.4
1.3	

1.3	1.2
1.3	x
1.3	1.2
1.3	1.2
1.3	1.2
1.3	1.2
1.3	x
1.3	x
1.3	x
1.3	x
1.3	x
1.4	
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	4.1
1.4	x
1.5	
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2

1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
1.5	4.2
2.0	
2.1	
2.1	2.1
2.1	2.1
2.1	2.1
2.1	x
2.1	2.1
2.1	2.1
2.1	2.1
2.1	2.1
2.1	2.1
2.1	x
2.1	2.1
2.1	2.1
2.1	2.1
2.1	2.2
2.1	2.2
2.1	2.2
2.1	x
2.1	2.1
2.1	2.1
2.1	2.2
2.1	3.5
2.1	x
2.1	2.2
2.2	
2.2	2.3
2.2	2.2
2.2	2.3
2.2	2.1
2.2	x
2.2	2.2
2.2	2.2
2.2	2.2
2.2	x
2.2	2.2
2.2	x
2.2	x
2.2	x
2.2	x
2.2	x
2.2	x
2.2	2.2
2.2	2.2
2.2	2.2

2.2	2.2
2.2	2.2
2.2	2.2
2.2	x
2.3	
2.3	5.2
2.3	5.2
2.3	5.2
2.3	5.2
2.3	5.2
2.3	5.2
2.3	5.1
2.3	5.1
2.3	5.1
2.3	5.1
2.3	5.1
2.3	5.1
2.3	5.1
2.3	5.1
2.4	
2.4	x
2.4	5.3
2.4	5.3
2.4	5.3
2.4	x
2.4	5.3
2.4	5.3
2.4	5.3
2.4	x
2.4	x
2.4	x
2.4	2.4
2.4	2.4
2.4	5.3
2.4	5.3
2.4	x
2.4	x
2.4	5.3
2.4	5.3
2.4	5.3
3.0	
3.1	
3.1	
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x

3.1	x
3.1	2.3
3.1	2.4
3.1	2.4
3.1	x
3.1	2.4
3.1	x
3.1	x
3.1	x
3.1	x
3.1	x
3.1	3.5
3.1	x
3.1	x
3.1	2.4
3.1	3.7
3.1	5.3
3.1	5.3
3.1	x
3.1	x
3.1	x
3.1	5.3
3.1	x
3.1	5.3
3.2	
3.2	
3.2	4.3
3.2	x
3.2	x
3.2	x
3.2	x
3.2	3.1
3.2	x
3.3	
3.3	3.6
3.3	3.2
3.3	x
3.3	3.6
3.3	x
4.0	
4.1	
4.1	4.3
4.1	x
4.1	4.1
4.1	x
4.1	2.1
4.1	2.1
4.1	x
4.1	x
4.1	3.5

4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.1	x
4.2	
4.2	3.5
4.2	3.2
4.2	x
4.2	3.x
4.2	3.1
4.2	x
4.2	3.1
4.2	x
4.2	2.2
4.2	5.3
4.2	5.3
4.2	5.3
4.2	5.3
4.2	5.3
4.2	5.3
4.2	5.3
4.2	x
4.2	5.3
4.2	5.3
4.3	
4.3	x
4.3	3.7
4.3	x
4.3	x
4.3	3.1
4.3	3.3
4.3	3.1
4.3	3.1
4.3	x
4.3	3.1
4.3	x
4.3	x
4.3	x
4.3	x
4.3	5.3
4.3	5.3

4.3	5.3
4.3	3.7
4.3	5.3
4.3	5.3
4.4	
4.4	3.3
4.4	x
4.4	x
4.4	3.4
4.4	x
4.4	x
4.4	x
4.4	x
4.4	x
4.4	x
4.4	x
4.4	5.3
4.4	x
4.4	x
4.4	x
4.4	3.7
4.4	3.7
4.4	3.7
4.4	3.7
4.5	
4.5	3.3
4.5	x
4.5	3.3
4.5	3.3
4.5	3.3
4.5	x
4.5	3.3
4.5	3.3
4.5	3.3
4.5	3.3
4.5	x
4.5	x
4.5	3.3
4.5	x
4.5	x
4.5	x
4.5	x
4.5	x
4.5	3.3
4.5	x
4.5	5.3
4.5	5.3
4.5	3.3
4.5	3.5

4.5	5.3
4.5	5.3
4.5	x
4.5	5.3
4.6	
4.6	3.4
4.6	3.4
4.6	x
4.6	3.4
4.6	3.7
4.6	x
4.6	3.4
4.6	3.4
4.6	x
4.6	x
4.6	x
4.6	x
4.6	x
4.6	x
4.6	x
4.6	5.3
4.6	x
4.6	x
4.6	x
4.6	5.3
4.6	x
4.7	
4.7	2.2
4.7	3.2
4.7	3.2
4.7	x
4.7	2.2
4.7	3.2
4.7	3.2
4.7	x
4.7	x
4.7	x
4.7	5.3
4.7	5.3
4.7	x
4.7	5.3
4.8	
4.8	3.6
4.8	3.6
4.8	3.6
4.8	3.6
4.8	x
4.8	3.6
4.8	3.6
4.8	3.2

4.8	3.6
4.8	3.6
4.8	3.4
4.8	3.6
4.8	x
4.8	x
4.8	x
4.8	5.3
4.8	5.3
4.8	5.3
4.8	5.3
4.8	5.3
4.9	
4.9	x
4.9	x
4.9	x
4.9	3.5
4.9	x
4.9	x
4.9	x
4.9	x
4.9	x
4.9	x
4.9	x
4.9	3.3
4.9	3.2
4.9	3.2
4.9	3.2
4.9	x
4.9	3.2
4.9	5.3
4.9	3.5
4.9	3.5
4.9	3.5
4.9	3.5
4.9	x
4.9	5.3
4.10	
4.10	5.2
4.10	5.3
4.10	x
4.10	x
4.10	x
4.10	5.2
4.10	x
4.10	x
4.10	5.2
4.10	5.3
4.10	5.3

4.10	x
4.10	x
4.10	x
4.10	x
5.0	
5.1	
5.1	3.7
5.1	3.7
5.1	3.7
5.1	3.7
5.1	x
5.1	3.7
5.1	x
5.1	x
5.1	3.7
5.1	x
5.1	3.7
5.1	x
5.1	x
5.1	x
5.2	
5.2	x
5.2	x
5.2	3.7
5.2	3.7
5.2	3.7
5.2	3.7
5.2	x
5.2	x
5.2	3.7
5.2	x
5.2	x
5.2	5.3
5.2	x
5.2	x
5.2	3.3
5.2	x
5.2	x
5.2	3.5
5.2	x
5.2	x
5.2	x
5.2	x
5.2	x
5.2	3.7
5.2	3.7
5.2	3.7
5.2	x
5.2	x
5.2	x

5.2	x
5.2	x
5.2	x
5.2	x
5.2	x
5.2	x
5.2	x
5.2	5.3
5.2	5.3
5.2	5.3
5.2	5.3
5.2	x
5.2	5.3
5.2	3.7
5.2	x
5.2	5.3
5.2	5.3
5.2	5.3
5.2	5.3
5.3	
5.3	3.7
5.3	3.7
5.3	3.7
5.3	x
5.3	x
5.3	x
5.3	x
5.3	x
5.3	x
5.3	x
5.3	x
5.3	x
5.4	
5.4	4.4
5.4	x
5.4	4.4
5.4	x
5.4	x
5.4	x
5.4	x
x	1.1
x	1.1
x	1.1
x	1.1
x	1.1
x	1.2
x	1.2
x	1.2
x	1.2
x	1.3
x	1.3

x	1.3
x	2.2
x	2.2
x	2.2
x	2.4
x	2.4
x	2.4
x	3.1
x	3.1
x	3.1
x	3.1
x	3.1
x	3.1
x	3.1
x	3.1
x	3.1
x	3.3
x	3.3
x	3.3
x	3.3
x	3.3
x	3.3
x	3.3
x	3.3
x	3.3
x	3.4
x	3.4
x	3.4
x	3.4
x	3.4
x	3.4
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.5

x	3.5
x	3.5
x	3.5
x	3.5
x	3.5
x	3.6
x	3.6
x	3.6
x	3.6
x	3.6
x	3.6
x	3.6
x	3.6
x	4.1
x	4.1
x	4.3
x	4.3
x	4.4
x	4.4

