GWAPT  Review

(Global Information Assurance Certification (GIAC) - Web Application Penetration Tester)

Src: https://www.giac.org/certification/web-application-penetration-tester-gwapt

GWAPT?

- Prüfung für den SANS 542 (Web Application Penetration Testing and Ethical Hacking)
  - SANS 542 - ~ $6.100
  - GWAPT (Prüfung) - ~ $1.699
    - Retakes - $ 729
    - Renewal - $ 429 + CPs (36 – 18 für OSCP) -> Erneuerung nach 4 Jahren notwendig

Src: https://www.giac.org/certifications/pricing & https://www.giac.org/certifications/renewal

SANS 542

Web Application Penetration Testing & Ethical Hacking

Src: https://www.sans.org/event/security-west-2018/course/web-app-penetration-testing-ethical-hacking

SANS 542.1 Introduction and Information Gathering

- Overview of the web from a penetration tester's perspective
- Exploring the various servers and clients
- Discussion of the various web architectures
- Discovering how session state works
- Discussion of the different types of vulnerabilities
- WHOIS and DNS reconnaissance
- The HTTP protocol
- WebSocket
- Secure Sockets Layer (SSL) configurations and weaknesses
- Heartbleed exploitation
- Utilizing the Burp Suite in web app penetration testing

SANS 542.2 Configuration, Identity and Authentication Testing

- Scanning with Nmap
- Discovering the infrastructure within the application
- Identifying the machines and operating systems
- Exploring virtual hosting and its impact on testing
- Learning methods to identify load balancers
- Software configuration discovery
- Learning tools to spider a website
- Brute forcing unlinked files and directories
- Discovering and exploiting Shellshock
- Web authentication
- Username harvesting and password guessing
- Fuzzing
- Burp Intruder

SANS 542.3 Injection

- Session tracking
- Authentication bypass flaws
- Mutillidae
- Command Injection
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- SQL injection
- Blind SQL injection
- Error-based SQL injection
- Exploiting SQL injection
- SQL injection tools
- sqlmap

SANS 542.4 XXE and XSS

- XML External Entity (XXE)
- Cross-Site Scripting (XSS)
- Browser Exploitation Framework (BeEF)
- AJAX
- XML and JSON
- Document Object Model (DOM)
- Logic attacks
- API attacks
- Data attacks

SANS 542.5 CSRF, Logic Flaws and Advanced Tools

- Cross-Site Request Forgery (CSRF)
- Python for web app penetration testing
- WPScan
- w3af
- Metasploit for web penetration testers
- Leveraging attacks to gain access to the system
- How to pivot our attacks through a web application
- Exploiting applications to steal cookies
- Executing commands through web application vulnerabilities
- When tools fail

GWAPT - Prüfung

- „Proctored Exam“ -> Pearson VUE – Testcenter
- Multiple-Choice - 75 Fragen
- 2 Zeitstunden (Optional: +15 Minuten Pause)
- Mind. 71% zum Bestehen
- Open Book
  - -> Dictionary (!)

Book.Page#	Specific Items	Short Description
1.5-1.10	Why the Web?	Book-Index
1.6	WebApps - Why?	larger attack surface, more complex, bigger pay-off
1.8	OSVDB	Open Source Vulnerability Database
1.9	AJAX	Asynchronous JavaScript and XML - Short Description
1.10	Cloud-Based Apps	Short Description
1.11-1.15	Understanding the Web	Book-Index
1.12	Pentesters Viewpoint	think malicious - act professinally, how to bypass restrictions, ...
1.13	Pen Test Methodology	Proven, Repeatable, Explainable
1.14	Knowledge of Tools	Gain in-depth knowledge, how to expand & improve them
1.16-1.22	Course Logistics	Book-Index
1.21	OTG	OWASP Testing Guide
1.22	OTG - Testing Categories	
1.23-1.28	Web App. Pen Tester's Toolkit	Book-Index
1.24	WebApps - Toolkit	Key considerations/items
1.25-1.26	Attack Platform	SamuraiWTF, Kali, Security542, ...
1.25	Kali	most popular penetration testing distribution
1.25	SamuraiWTF	for Web Penetration Testing
1.25	Security542	custom Xubuntu-based VM
1.26	kali-linux-web	Kali Linux Web Metapackage
1.27	WebApp Security Scanner	highly automated, push-button, webapp security scanner
1.27	Network Vuln. Scanner	determine what app or serivce are running & current patch level
1.28	Browsers	
1.29-1.51	Interception Proxies	Book-Index
1.30	Interception Proxies	Short Description
1.31	Interception Tools	can analyze traffic & inject attacks
1.32	Interception Methods	sniffers, interception proxy, HTTPS issues
1.32	Sniffers	capture traffic on the same network as the device
1.32	Interception Proxy	configure the device to connect to the proxy or interception machine

Book.Page#	Specific Items	Short Description
3.64	"%00"	the C string handling that treats a null as the end of the string (%00)
3.49	&&	run the 2nd command if the first command exits without error
1.124	.htaccess	can be removed by Method DELETE
3.49	;	run the 2nd command after the first command (regardless of any errors)
4.61	9zqjx	Magic reflection string is used to try to discover potentially reflected input & locate where within the source
3.14	abcdefg	crypted with Base64-encoded, md5sum and hex-encoded
1.9	AJAX	Asynchronous JavaScript and XML - Short Description
4.129-4.140	AJAX	Book-Index
4.138	AJAX - Attack Surface	surface is larger than "normal" apps - large amounts of client-side code - business logic is client side
4.140	AJAX - Exploitation	not more difficult for AJAX apps, as long as we understand how the flaw fits within the app
4.130	AJAX - Introduction	Asynchronous JavaScript and XML - Short Description
4.139	AJAX - Mapping	many tools cannot parse & handle client-side logic - main difficulty is caused by links being dynamically generated
4.137	AJAX - Mash-Up - Proxy Issues	control of the URLs to proxy
4.134	AJAX - Mash-Ups	combining two or more apps to provide a larger feature set - same origin causes issues -> proxy capabilities
4.132	AJAX - readyState	five possible values: 0-4
4.135-4.137	AJAX - Same Origin	does not change the same origin policy -> use a proxy built in to their app
4.133	AJAX - XMLHttpRequest - Example	Example
1.37,1.46	AJAX Spider	(potentially) discover additional dynamic content (ZAP,BURP)
2.55	AJAX Spider	to contend with client-side dynamically generated link-problems
4.131	AJAX -XMLHttpRequest	Short Intro
2.76-2.81	Analyzing Spidering Results	Book-Index
2.77	Analyzing Spidering Results: What to look for	Comments+commented code&links, disabled functionality, linked servers
2.111	Apache	/images
2.139	Apache mod_auth_digest	Short Description
2.12	Apache mod_security module	to change the server "Prod" string
4.141-4.146	API Attacks	Book-Index
4.146	API Attacks - Exploiting Framework Flaws	call functions without authentication, may gather information, exploit of complex code that hasn't been updated
4.143	API Attacks - Framework Files	most commonly considered files are JavaScript files

GWAPT - Prüfung

- „Proctored Exam“ -> Pearson VUE – Testcenter
- Multiple-Choice - 75 Fragen
- 2 Zeitstunden (Optional: +15 Minuten Pause)
- Mind. 71% zum Bestehen
- Open Book
  - -> Dictionary (!)

- 2 Testläufe

GIAC Web Application Penetration Tester (GWAPT)

Name [redacted]
Account ID [redacted]

Completed February 16th, 2018
Exam ID [redacted]

GWAPT Practice Test

Score: 71%

Status: Passed

Cross Site Request Forgery, Cross Site Scripting and Client Injection Attack	★★★★☆
Reconnaissance and Mapping	★★★★☆
Web Application Authentication Attacks	★★★☆☆
Web Application Configuration Testing	★★★★☆
Web Application Overview	★☆☆☆☆
Web Application Session Management	★★★★☆
Web Application SQL Injection Attacks	★★★★☆
Web Application Testing Tools	★★★☆☆

GWAPT – Prüfung ohne SANS 542?

- Möglich, aber …

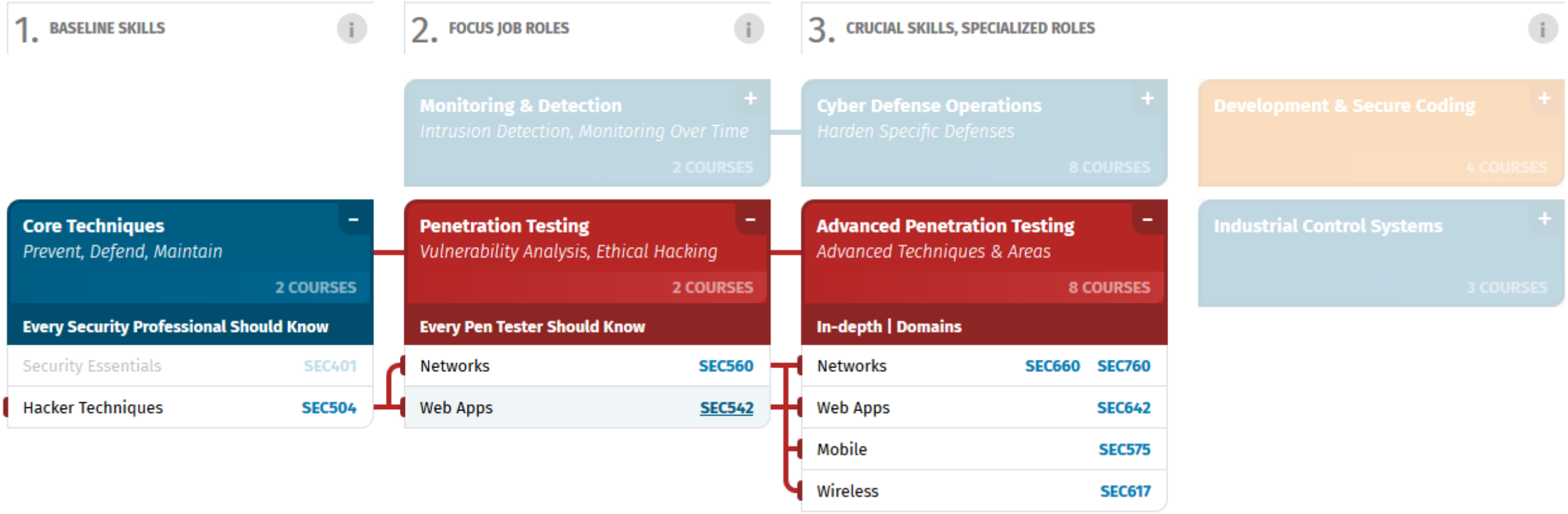
- Nicht für Anfänger!
  - Fragen teilweise sehr speziell
    - SQLi: Sleep(10) / WAITFOR DELAY ´0:0:10´
      - Welches DBMS wurde angegriffen?
    - Welche Applikation benötigt einen Haufen an API-Keys?
      - Recon-ng (?)
    - Spezielle Python-Fehlermeldungen
      - Nur lösbar, wenn man sich mit Python einigermaßen auseinandergesetzt hat

SANS 542 vs. OSCP (?)

- SANS 542
  - Web Application-lastig -> SANS 560 (Networks)
  - Angeleitet – Fester Ramen (straight Forward)
  - Basics - Anfängerfreundlich

- OSCP
  - Netzwerk-lastig
  - “Ins kalte Wasser geschmissen” – Sehr weit gefasster Ramen
  - Viel Eigeninitiative notwendig – nicht sehr Anfängerfreundlich

Was kommt danach?



Src: https://www.sans.org/cyber-security-skills-roadmap