CNWPP - Certified Network & Web app Pentesting Professional

https://thexssrat.podia.com/0d8525b0-a43e-448a-b003-efee5061432e/

001. Defining what a pentest is

001 - 1 Defining a pentest

001 - 2_assignment_-*defining_a_pentest*

001 - 3 The deliverables of pentesting

001 - 3 ASSIGNMENT The deliverables of pentesting

001 - 4 The pentest plan

001 - 5 Assignment_Make_a_test_plan_for_hackxpert.com

001 - 5 SOLUTION Assignment_Make_a_test_plan_for_hackxpert.com

001 - 6 EXAMPLE the_pentesting_report

001 - XTRA1 The methodologies of a pentest

001 - XTRA2 - Letter of pen test commencing

001 - XTRA3 - SHORT TEST PLAN - UNCLE RAT'S EXAMPLE

001 - XTRA4 - The NDA

002. The pentesting methodologies

002.1 Pentesting methodolgies

002.2 Assignment - describe the methodologies in your own words

002.3 - 001 OSSTMM

002.3 - 006 RAV CALC_OSSTMM

002.4 OWASP methodology

002.5 OSSTMM assignment

002.6 OWASP assignment

002.8 PTES - Pre-engagement

002.8 PTES Questionaires for pentests

002.9 PTES Information gathering

003. Network scanning and exploits

003.1 BIS - How we do a pentest

003.2 Nmap (1)

003.2 port scanning

003.3 portscanning assignment (1)

003.4 FTP (1)

003.5 FTP assignment (1)

003.6 SMB (1)

003.7 EXPLOIT-DB network hacking tools (1)

003.7 network hacking tools (1)

003.7 WIRESHARK network hacking tools (1)

003.8 DEMO Nikto Nmap network hacking tools assignment (1)

003.8 network hacking tools assignment (1)

004. Web exploits pt. 1

004.1 Fuzzing

004.1.1 Fuzzing Assignment

004.2 Burp Suite CE

004.3 CSRF

004.3 CSRF CHECKLIST

004.3 CSRF Source code

004.4 CSRF assignment

004.5 JWT CHECKLIST

004.5 JWT

004.6 JWT assignment

004.6 SOLUTION JWT assignment

004.7 Open redirect

004.8 Open redirects assignment

004.9 SSRF

004.10 SSRF LABS

004.11 SSRF labs solutions

005. Web exploits pt. 2

005.1 IDOR - Slides

005.1.1 BAC - In-depth demo

005.1.2 IDOR - Demo manual exploitation

005.1.3 IDOR - Demo Authorize exploitation

005.2 IDOR AND BAC LABS

005.3 Business logic flaws

005.4 LABS BUSINESS LOGIC FLAWS

005.5 captcha bypasses

005.6 captcha labs

005.7 XPATH injections

005.7.1 XPATH injections labs

005.8 Insecure_deserialization

006. Methodologies

006.1 A_main app_methodology_V5.0 (1)

006.2 Broad scope methodology (1)

006.3 Broad_scope_methodology_-_Manual (2)

006.XTRA1 Practical_demonstration_-_Main_application_hacking (1) (1)

006.XTRA2 Broad Scope Methodology

006.XTRA3 Extra Resources - Main app methdology

006.XTRA4 Main app methodology (1)

007. Vulnerability scanners & tools

007.1 Vulnerability scanners

007.2 vulnerability scanners ASSIGNMENTS

007.3 out of band servers

007.4 Labs out of band server

007.5 Postman demo

007.6 postman labs

007.7 Assignement- scan hackxpert with zap

008. The OWASP top 10 + WAFs

008.1 OWASP top

008.2 OWASP API top 10

008.3 OWASP Mobile top 10

008.4 Web_Application_Firewalls_(WAFs)_Form_A_to_Z (1)

008.5 WAF_evasion_techniques_checklist (1)

008.XTRA1 two-armed mode WAF

009. Advanced web exploits

009.1 XSS

009.2 XSS labs

009.3 CSP

009.4 CSP excercises

009.5 CSP labs

009.7 hack me labs - Pentest simulation of exploitation phase

010. Exam day - Plan within 6 months

- Prove your might in this tough exam that will test your skills and patience!
- You will get a seperate environment to hack
- You will be expected to evade filters
- You will be expected to submit a test plan, notice of engagement, test report and give me a debriefing
- You get 8 hours to hack
- You get 24 hours after hacking to submit the report

- You get 24 hours after hacking to submit the debrief
- You will be expected to hack a web app, the server itself and an API
- To pass you will be expected to identify at least 30 vulnerabilities ranging from low to critical. There are more but how many exactly is not public information.
- This exam is not for the faint of heart