COMPTIA PENTEST+ - TIPS AND TRICKS

JOAS ANTONIO

DETALHES

- Esse documento foi feito para ajudar e auxiliar profissionais na área de segurança que estão em busca dessa certificação, por conta disso eu reunir bastante informações e consultei alguns profissionais que possuem a certificação.
- Mas é claro que só com isso não garante que você passe na prova
- Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

ADQUIRINDO FOCO

- Primeiramente é necessário adquirir um foco para estudar para certificação,
- principalmente se você deseja ir bem e tirar proveito do conteúdo ao máximo. Então
- técnicas como pomodoro e pirâmide de aprendizagem é muito bom, eu recomendo em sua
- jornada fazer isso, vale para qualquer certificação.
- ● Deixe o telefone de lado para estudar;
- ● Foque somente em um módulo por vez;
- ● Faça anotações manuais ou até desenhos e rascunhos;
- ● Procure por questões práticas que ajude você a se desenvolver mais;
- ● E na dúvida, reveja o material ou procure outras fontes de conhecimento para ter total
- entendimento daquilo que você está estudando;

LIVROS E EBOOKS PARA ESTUDO

- https://www.amazon.com.br/CompTIA-PenTest-Certification-Guide-PT0-001/dp/1260135942/ref=asc_df_1260135942/?tag=googleshopp00-20&linkCode=df0&hvadid=379726160779&hvpos=&hvnetw=g&hvrand=17919455106519665927&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001773&hvtargid=pla-529461746572&psc=1
- https://www.amazon.com.br/CompTIA-PenTest-Certification-PT0-001-English-ebook/dp/B07PKS785B/ref=asc_df_B07PKS785B/?tag=googleshopp00-20&linkCode=df0&hvadid=379725882390&hvpos=&hvnetw=g&hvrand=17919455106519665927&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001773&hvtargid=pla-865602654647&psc=1
- https://www.amazon.com/CompTIA-PenTest-Practice-Tests-PT0-001/dp/1119542847
- https://www.amazon.com/CompTIA-PenTest-Certification-Practice-PT0-001/dp/1260440907/ref=sr_1_6?dchild=1&keywords=pentest%2B&s=books&sr=1-6
- amazon.com/CompTIA-PenTest-Cert-Guide-Certification-ebook/dp/B07KKM68QV?pldnSite=1

AWESOME AND CHEATSHEET

- Além dos livros, você pode usar o Exam Guide para consultar o que cai na prova e estudar através de materiais também disponibilizados na internet
- Pesquise por pentest+ exam guide filetype:pdf
- https://github.com/dustypioneer/pentest_plus
- https://github.com/pentestplus
- https://github.com/PacktPublishing/CompTIA-Pentest-Ethical-Hacking-Course-and-Practice-Exam
- https://github.com/xChockax/CompTIA-Pentest-PT0-001
- https://github.com/PacktPublishing/CompTIA-PenTest-Exam-Guide-PT0-001
- https://github.com/PacktPublishing/-Ethical-Hacking-and-CompTIA-PenTest-Exam-Prep-PT0-001-
- https://pentestplus.github.io/
- https://github.com/artiommocrenco/comptia-pentest-notes

DICAS

- Estude bastante vetores de ataques em aplicações web, pois cai muitas perguntas voltadas a técnicas e até mesmo remediações, envolvendo a parte de segurança de aplicação web, por exemplo: Como impedir um SQL Injection ou LFI?
- Além disso, conhecer de frameworks e metodologias de PenTest é fundamental, pois cai questões envolvendo um ciclo de pentest de tal metodologia;
- Conhecer de nmap é fundamental também, cai bastante perguntas sobre a ferramenta e explorar todas as suas sintaxes pelo menos saber para que serve cada um já é o suficiente;
- Entender de vetores de ataques voltados a Engenharia Social, pois você vai se deparar com muitas questões que trazem cenários e situações;
- Conhecer um pouco dos fundamentos envolvendo segurança de aplicação e hardening, também é interessante, pois cai questões que você pode precisar mitigar ou realizar algum hardening ou até mesmo code review;
- Conhecer as principais ferramentas utilizadas no mercado e fundamental;
- Conhecer as técnicas envolvidas em cada ciclo de PenTest, desde a coleta de informação ate o relatório;
- Vai cair bastante questão que pode questionar quais ações você deve tomar, ao se deparar com alguma inconformidade e etc;
- Eu recomendo anotar conceitos, nomenclaturas e jargões que cai muito na prova, por exemplo: SOW, NDA e etc...

CURSOS

- Eu recomendo fazer cursos, principalmente para te preparar tanto teoricamente como tecnicamente, existem diversos na Udemy ou instituições parceiras da CompTIA que oferecem;
- Ou comprar diretamente o material oficial e estudar em cima dele e claro, comprar laboratórios para você por em prática suas habilidades;

SIMULADOS

- https://issuu.com/freedumpsquestions2019/docs/comptia_pentest__pt0-001_free_dumps_questions_v9.0
- https://www.youtube.com/watch?v=s6yehzNuD5M&ab_channel=PacktVideo
- https://www.edusum.com/category/pentest-plus-simulator
- https://www.mindomo.com/pt/outline/how-are-you-able-to-clear-pt0-001-exam-with-pt0-001-test-simulator-and-exam-dumps-94e7bf0a42fc43948565af6a6a985b1f
- https://www.udemy.com/course/comptia-pentest-pt0-001-practice-tests-4-exams/
- https://www.udemy.com/course/ethical-hacking-and-comptia-pentest-exam-prep-pt0-001/
- https://www.udemy.com/course/practice-comptia-pentest-exam-340-questions-pt0-001/
- Esse são alguns simulados que podem ajudar, mas não significa que as questões apresentadas vão cair na prova

LABORATÓRIOS

- https://tryhackme.com/path/outline/pentestplus
- https://www.cybrary.it/catalog/practice_labs/comptia-pentest-plus/
- https://www.reddit.com/r/CompTIA/comments/eehi5y/pentest_labs/
- https://www.hackthebox.eu/
- http://vulnhub.com/

PROCESSO DE REALIZAÇÃO DA PROVA

- Se a prova não possuir na língua nativa, você provavelmente vai ter um proctor americano para supervisionar sua prova;
- Teste de sistema no computador e na rede em que você planeja fazer o exame;
- Identificação necessária (emitida pelo governo);
- Assine um NDA (acordo de não divulgação) antes do teste;
- Navegador de bloqueio ativado;
- Apresente todo o seu ambiente de trabalho ao inspetor antes do teste;
- Requer webcam (o vídeo é gravado e o inspetor está observando você);
- Sem ruídos perturbadores;
- Sem pausas para ir ao banheiro;
- Sem comida (apenas bebidas permitidas são água em um copo transparente);
- Não tem permissão para deixar sua cadeira em QUALQUER MOMENTO durante o exame;

REVIEWS DA PROVA

- https://medium.com/@kcco.io/comptia-pentest-certification-exam-review-1a0a02883650
- https://www.tevora.com/comptia-pentest-certification-review/
- https://www.reddit.com/r/CompTIA/comments/8er30w/i_took_pentest_today_and_even_as_a_pentester_that/
- https://resources.infosecinstitute.com/topic/pentest-plus-vs-ceh/
- https://www.youtube.com/watch?v=I12oxXncQCE&ab_channel=I.T.CareerQuestions
- https://www.youtube.com/watch?v=nUXL39z91k4&ab_channel=Infosec
- https://medium.com/@h4unt3r/comptia-pentest-certification-review-4ce42871e39b
- https://blog.wyatttauber.com/how-i-passed-comptia-pentest-pt0-001-75471e505abd
- https://www.linkedin.com/pulse/my-comptia-pentest-study-guide-kelshall-williams/?articleId=6652888150140088322