CEH Fundamentals

Prof. Joas Antonio

Sobre o Livro

- Esse livro é apenas um acervo de links e tutoriais sobre cada área do CEH
- O objetivo não é apresentar nenhum conceito, pois já existem livros mais completos e feito por profissionais que possuem a certificação e são instrutor da mesma
- E você pode procurar os cursos da ACADI-TI, Udemy, Cybrary e Ucertify sobre o CEH, aonde vai desde de cursos até simulados

Sobre o Autor

- Joas Antonio
- Cyber Security Analyst, Cyber and Information Security Consultant by Betta GP, Information Security Researcher by Experience Security, Ethical Hacking and PenTest, OWASP Member and Researcher, Cybrary Teacher Assistant, Microsoft Instructor, Web Developer, Bug Hunter by HackerOne and OBB, Python Developer, has over +300 technology courses and +31 certifications, SANS Member, CIS Member and Research, Cyber Security Mentor and IT lover.

Introdução ao Ethical Hacking

O que é um Hacker Ético?

- Um **Hacker Ético** é um especialista em sistemas e redes de computadores que conhece as técnicas e métodos utilizados para se encontrar vulnerabilidades de segurança em softwares e redes corporativas.
- No entanto, ao invés de usar esse conhecimento para obter vantagem própria, ele apenas documenta as vulnerabilidades detectadas e as reporta para a empresa que está contratando seus serviços, juntamente com indicações de como solucionar as vulnerabilidades e aumentar a segurança da corporação.
- Vulnerabilidades de segurança são encontradas em má implementação de softwares, sistemas e dispositivos mal configurados, ausência de sistemas de seguranca como Firewalls, ou até mesmo softwares desatualizados. A função do Ethical Hacker é encontrar essas falhas utilizando-se de técnicas de intrusão, porém sem causar nenhum impacto nos sistemas.

O que é um PenTest

- O termo PenTest é derivado de **Penetration Test**, em português a melhor tradução seria Testes de Intrusão ou de Invasão.
- O PenTest é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas. Através dessas técnicas, o profissional **Pentester** irá identificar as vulnerabilidades existentes na arquitetura da empresa, explorá-las e entregar um relatório à empresa, que deverá então tomar as devidas ações para corrigir as falhas de segurança.
- Apesar de ser uma simulação de um ataque hacker, é importante mencionar que o PenTest é uma atividade profissional e sobretudo ética. Uma empresa contrata esses serviços para ter seus sistemas analisados por uma empresa ou profissional qualificado.
- Um Pentest não é apenas um scaneamento de portas e vulnerabilidades, ele vai além disso. O Pentest faz uso de softwares e ferramentas (pentest tools) para explorar as vulnerabilidades identificadas, buscando identificar que tipo de informação pode ser obtida através daquela falha.

Tipos de PenTest

- **Black box**
- Em um ataque cibernético do mundo real, o hacker provavelmente não conhecerá todos os meandros da infraestrutura de TI de uma corporação. Por isso, ele ou ela lançará um ataque de força bruta total contra a infraestrutura de TI, na esperança de tentar encontrar uma vulnerabilidade ou fraqueza na qual se prendem.
- Em outras palavras, nesse tipo de Teste de Caneta, não há informações fornecidas ao testador sobre o funcionamento interno de um Aplicativo Web específico, nem sobre seu código fonte ou arquitetura de software. Como resultado, esse tipo de teste específico pode levar muito tempo para ser concluído; muitas vezes, o testador dependerá do uso de processos automatizados para descobrir completamente os pontos fracos e vulnerabilidades. Esse tipo de teste também é chamado de abordagem de "tentativa e erro".

Tipos de PenTest

- **White box**
- Nesse tipo de teste de caneta, também conhecido como "Clear Box Testing", o testador tem conhecimento e acesso completos ao código-fonte e à arquitetura de software do aplicativo Web. Por esse motivo, um teste de caixa branca pode ser realizado em um período de tempo muito mais rápido quando comparado a um teste de caixa preta. A outra vantagem disso é que um Teste de Caneta muito mais completo pode ser concluído.
- Mas, essa abordagem também tem seu conjunto de desvantagens. Primeiro, como um testador possui conhecimento completo, pode levar mais tempo para decidir sobre o que focar especificamente em relação aos testes e análises de sistemas e componentes. Segundo, para realizar esse tipo de teste, são necessárias ferramentas mais sofisticadas, como as dos analisadores e depuradores de código de software.

Tipos de PenTest

- **Gray box**
- Como o nome indica, esse tipo de teste é uma combinação dos testes Black Box e White Box. Em outras palavras, o testador de penetração possui apenas um conhecimento parcial do funcionamento interno dos aplicativos da Web. Isso geralmente é restrito a apenas obter acesso ao código do software e aos diagramas de arquitetura do sistema.
- Com o Gray Box Test, os processos de teste manual e automatizado podem ser utilizados. Devido a essa abordagem, o testador de caneta pode concentrar seus esforços principais nas áreas do aplicativo Web sobre as quais ele mais conhece e, a partir daí, a partir daí, explorar quaisquer pontos fracos ou vulnerabilidades. Com esse método específico, há uma probabilidade maior de que também sejam descobertas “brechas de segurança” mais difíceis de encontrar.

Metodologias de PenTest

- **Reconhecimento:**

O reconhecimento é onde você coleta informações sobre seu alvo. Você deseja entender o escopo do seu empreendimento antecipadamente, é claro. Isso o ajudará a restringir suas ações, para que você não se envolva em nada que possa ser antiético. Você terá uma noção de quem é seu alvo, mas pode não ter todos os detalhes. Reunir os detalhes do seu alvo é uma das razões para realizar o reconhecimento. Outro motivo é que, embora exista muita informação que deve ser pública apenas devido à natureza da Internet e à necessidade de fazer negócios lá, você pode encontrar informações vazadas para o resto do mundo em que a organização para a qual você está trabalhando faria melhor para bloquear.

- **Scanning e Enumeração:**

Depois de identificar os blocos de rede, você desejará identificar os sistemas acessíveis nesses blocos de rede; esse é o estágio de varredura e enumeração. Mais importante, no entanto, você desejará identificar serviços em execução em qualquer host disponível. Por fim, esses serviços serão usados como pontos de entrada. O objetivo é obter acesso, e isso pode ser possível por meio de serviços de rede expostos. Isso inclui não apenas uma lista de todas as portas abertas, que serão informações úteis, mas também a identidade do serviço e software em execução atrás de cada porta aberta.

Metodologias de PenTest

- **Exploração:**

Obter acesso é o que muitas pessoas consideram ser a parte mais importante de um teste de penetração e, para muitos, é o mais interessante. É aqui que você pode demonstrar que alguns serviços são potencialmente vulneráveis. Você faz isso explorando o serviço. Não há positivos teóricos ou falsos quando você comprometeu um sistema ou roubou dados e pode prová-lo. Isso destaca um dos aspectos importantes de qualquer hacking ético: a documentação. Apenas dizer: "Ei, eu fiz isso" não será suficiente. Você precisará demonstrar ou provar de alguma forma que conseguiu comprometer o sistema.

- **Pós Exploração:**

Quando você entra, emular padrões comuns de ataque significa que você deve manter o acesso. Se você conseguiu comprometer o sistema de um usuário, quando o usuário desligar o sistema, você perderá o acesso. Isso pode significar que você precisará comprometer novamente o sistema. Como nem sempre é garantido que as explorações são eficazes, é possível que você não consiga entrar na próxima vez que tentar a exploração. Além disso, você pode ter usado uma exploração que dependia de uma vulnerabilidade que foi corrigida. Sua próxima tentativa pode falhar porque a vulnerabilidade não está mais lá. Você precisa se dedicar a outros meios de entrar no sistema para ter certeza de manter a capacidade de ver o que está acontecendo nesse sistema e potencialmente na rede corporativa em geral.

Fundamentos de Redes

Modelos de comunicação

- http://masimoes.pro.br/redes-de-computadores/introducao/padroes-de-comunicacao.html
- http://w3.ufsm.br/natanael/ComDadosUFSM/ComDados16.pdf
- https://pt.wikipedia.org/wiki/Modelo_OSI
- https://www.teleco.com.br/tutoriais/tutorialsnmpred1/pagina_2.asp

Topologias

- https://pt.wikipedia.org/wiki/Topologia_de_rede
- https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens
- https://www.youtube.com/watch?v=XcK_kZxs65A
- https://br.ccm.net/contents/258-topologia-de-redes
- http://producao.virtual.ufpb.br/books/camyle/introducao-a-computacao-livro/livro/livro.chunked/ch07s03.html

Rede física

- https://www.ibm.com/support/knowledgecenter/pt-br/SSPHQG_7.2/concept/ha_concepts_physical_logical.html
- https://siteantigo.portaleducacao.com.br/conteudo/artigos/informatica/topologia-fisica-das-redes-de-computadores/29017
- https://www.portalgsti.com.br/2017/07/redes-logicas.html
- https://www.youtube.com/watch?v=YcjX-rzg9Sc

Protocolos de Rede

- https://www.opservices.com.br/protocolos-de-rede/
- https://pt.wikipedia.org/wiki/Lista_de_protocolos_de_redes
- https://pt.wikipedia.org/wiki/Protocolo_(ci%C3%AAncia_da_computa%C3%A7%C3%A3o)
- https://www.youtube.com/watch?v=6-RzPthCSns
- http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_inf/081112_protserv_redes.pdf
- https://www.uniaogeek.com.br/o-que-e-um-protocolo-de-redes/

Arquitetura de redes

- https://pt.wikipedia.org/wiki/Arquitetura_de_rede
- https://www.youtube.com/watch?v=Pg_Xv0EnkWo
- https://pt.wikibooks.org/wiki/Redes_de_computadores/Arquitetura_de_redes_de_computadores
- http://docente.ifrn.edu.br/helbersilva/disciplinas/arquitetura-redes/aula-1/view
- https://web.fe.up.pt/~mricardo/02_03/rcd/teoricas/arquitecturas_v4.pdf

Introdução ao Reconhecimento e Enumeração

Ferramentas de Reconhecimento e Enumeração

- https://osintframework.com/
- https://www.youtube.com/watch?v=SzNpnZ_cqrw
- https://www.youtube.com/watch?v=XdNjPVLlLNA
- https://www.sans.org/security-resources/GoogleCheatSheet.pdf
- https://cdn5.alienvault.com/blog-content/GoogleHackingCheatSheet.pdf
- https://gbhackers.com/latest-google-dorks-list/
- https://hackertarget.com/maltego-transforms/
- https://ismart.unm.edu/files/7113/8379/8002/maltego.pdf
- https://www.hackingloops.com/maltego/
- https://pentest-tools.com/information-gathering/website-reconnaissance-discover-web-application-technologies
- https://securitytrails.com/blog/top-20-intel-tools
- https://thehackerstuff.com/top-10-advanced-information-gathering-tools-for-linux-windows/

Ferramentas de Reconhecimento e Enumeração

- https://www.tutorialspoint.com/kali_linux/kali_linux_information_gathering_tools.htm
- https://securitytrails.com/blog/information-gathering
- http://literacybasics.ca/strategic-planning/strategic-planning-assesssment/overview-and-information-gathering-tools/
- https://medium.com/webeagle/information-gathering-tools-for-maximum-cybersecurity-78ef3212773f
- http://www.yourarticlelibrary.com/management/mis-management/tools-of-information-gathering-for-system-analysis/70398
- https://www.armourinfosec.com/online-information-gathering-tools/
- https://resources.infosecinstitute.com/information-gathering/#gref
- https://github.com/topics/information-gathering-tools

Introdução ao Scanning

Ferramentas de Scanning

- https://securitytrails.com/blog/best-port-scanners
- https://geekflare.com/port-scanner-tools/
- https://geekflare.com/find-wordpress-vulnerabilities/
- https://wpscan.org/
- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- https://www.dnsstuff.com/network-vulnerability-scanner
- https://hackertarget.com/vulnerability-scanner/
- https://www.softwaretestinghelp.com/penetration-testing-tools/
- https://www.guru99.com/top-5-penetration-testing-tools.html
- https://www.esecurityplanet.com/products/top-penetration-testing-tools.html

Introdução ao System Hacking

Ferramentas e métodos para System Hacking

- https://blog.compass-security.com/2019/10/hacking-tools-cheat-sheet/
- https://github.com/kobs0N/Hacking-Cheatsheet
- https://www.dummies.com/computers/computer-networking/network-security/hacking-for-dummies-cheat-sheet/
- http://index-of.co.uk/Google/Hacking%20-%20CEH%20Cheat%20Sheet%20Exercises.pdf
- https://br.pinterest.com/pin/389209592781638234/
- http://xeushack.com/the-ultimate-hacking-cheat-sheet
- https://medium.com/oscp-cheatsheet/oscp-cheatsheet-6c80b9fa8d7e
- https://github.com/so87/OSCP-PwK
- https://github.com/P3t3rp4rk3r/OSCP-cheat-sheet-1
- https://xmilkpowderx.github.io/2019-05-16-OSCPCheatSheet/
- https://sushant747.gitbooks.io/total-oscp-guide/

Ferramentas e métodos para System Hacking

- https://nitesculucian.github.io/2018/12/01/metasploit-cheat-sheet/
- https://www.comparitech.com/net-admin/metasploit-cheat-sheet/
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Metasploit%20-%20Cheatsheet.md
- https://pentestmag.com/metasploit-cheat-sheet/
- https://pentesttools.net/metasploit-cheat-sheet/
- https://resources.infosecinstitute.com/metasploit-cheat-sheet/
- https://0xsecurity.com/blog/some-hacking-techniques/post-exploitation-cheat-sheet
- https://github.com/kmkz/Pentesting/blob/master/Post-Exploitation-Cheat-Sheet
- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List
- https://medium.com/@int0x33/day-26-the-complete-list-of-windows-post-exploitation-commands-no-powershell-999b5433b61e

Ferramentas e métodos para System Hacking

- https://pentest.tonyng.net/windows-post-exploitation-command-list/
- http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf
- https://www.exploit-db.com/docs/english/26000-windows-meterpreterless-post-exploitation.pdf
- https://www.guru99.com/how-to-crack-password-of-an-application.html
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/
- https://www.itpro.co.uk/security/34616/the-top-ten-password-cracking-techniques-used-by-hackers
- https://blog.focal-point.com/lets-get-cracking-a-beginners-guide-to-password-analysis
- https://www.owasp.org/images/e/e0/OWASPBristol-2018-02-19-practical-password-cracking.pdf
- https://www.freecodecamp.org/news/an-intro-to-password-cracking/

Introdução a Malwares

Malware (Types and Analysis)

- https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
- https://www.lastline.com/blog/malware-types-and-classifications/
- https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html
- https://www.geeksforgeeks.org/malware-and-its-types/
- https://www.upguard.com/blog/types-of-malware
- https://en.wikipedia.org/wiki/Malware_analysis
- https://www.hybrid-analysis.com/
- https://www.sans.org/reading-room/whitepapers/malicious/paper/2103
- https://digital-forensics.sans.org/media/malware-analysis-cheat-sheet.pdf
- https://zeltser.com/malware-analysis-cheat-sheet/

Malware (Types and Analysis)

- https://www.andreafortuna.org/2016/08/16/cheat-sheet-for-malware-analysis/
- https://www.reddit.com/r/Malware/comments/3zpkgm/reverse_engineering_for_malware_analysis_cheat/
- https://www.dfir.training/cheat-sheets
- https://www.youtube.com/watch?v=tgJR1-mkvzY
- https://www.first.org/global/sigs/malware/resources/

Malware (Create and Infraestructure)

- https://zeltser.com/cheat-sheets/
- https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-1/
- https://niiconsulting.com/checkmate/2018/02/malware-development-welcome-dark-side-part-2-1/
- https://github.com/topics/malware-development
- https://medium.com/@rwxrob/modern-malware-development-languages-70facadecd8
- https://www.youtube.com/watch?v=9m7NtP5HdHI
- https://www.youtube.com/watch?v=nhYR0F7seMs
- https://www.youtube.com/watch?v=fv4l9yAL2sU
- https://thenextweb.com/security/2019/08/06/malware-attacks-on-infrastructure-and-state-run-facilities-shot-up-200-in-2019/

Introdução ao Sniffing e Spoofing

Sniffing and Spoofing

- https://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/
- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/
- https://hackertarget.com/wireshark-tutorial-and-cheat-sheet/
- https://www.dicas-l.com.br/download/tcpdump-cheat-sheet-1.pdf
- https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c
- https://courses.cs.washington.edu/courses/cse461/13wi/lectures/WiresharkSection.pdf
- https://www.youtube.com/watch?v=visrNiKIP3E
- https://isc.sans.edu/forums/diary/Packet+Analysis+Where+do+you+start/22001/
- https://pt.slideshare.net/y3dips/packet-analysis
- https://pt.slideshare.net/y3dips/packet-analysis

Sniffing and Spoofing

- https://en.wikipedia.org/wiki/Spoofing_attack
- https://www.malwarebytes.com/spoofing/
- https://github.com/Sab0tag3d/MITM-cheatsheet
- https://owasp.org/www-community/attacks/Content_Spoofing
- https://blackarch.org/spoof.html
- https://www.veracode.com/security/spoofing-attack
- https://www.sciencedirect.com/topics/computer-science/spoofing-attack
- https://www.comparitech.com/net-admin/spoofing-attacks-guide/

Introdução a Engenharia Social

Engenharia Social

- https://www.social-engineer.org/framework/se-tools/
- https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/
- https://github.com/trustedsec/social-engineer-toolkit
- https://medium.com/@nancyjohn_95536/using-set-tool-kit-to-perform-website-cloning-in-kali-linux-67fa01c92af9
- https://www.infinityinc.us/attack-of-the-clones-how-to-avoid-the-website-cloning-trap/
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/
- https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/
- https://resources.infosecinstitute.com/top-9-free-phishing-simulators/
- https://www.skyhighnetworks.com/cloud-security-blog/top-phishing-test-tools-and-simulators/
- https://github.com/topics/phishing

Engenharia Social

- https://en.wikipedia.org/wiki/Social_engineering_(security)
- https://www.social-engineer.org/
- https://www.webroot.com/au/en/resources/tips-articles/what-is-social-engineering
- https://fossbytes.com/what-is-social-engineering-types-techniques/
- https://www.datto.com/uk/blog/5-types-of-social-engineering-attacks
- https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
- https://phoenixnap.com/blog/what-is-social-engineering-types-of-threats
- https://www.pivotpointsecurity.com/blog/physical-social-engineering-attacks/
- https://rhinosecuritylabs.com/social-engineering/business-prepared-person-social-engineering-attack/
- https://builtin.com/cybersecurity/what-is-social-engineering
- https://www.social-engineer.org/framework/information-gathering/physical-methods-of-information-gathering/

Introdução a Wireless Hacking

Wireless Hacking

- https://www.aircrack-ng.org/doku.php?id=simple_wep_crack - https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/ - https://medium.com/infosec-adventures/crack-wep-key-with-a-connected-client-e78348bec8a8 - https://www.youtube.com/watch?v=Wu2MQW9H8HQ - https://www.youtube.com/watch?v=Wu2MQW9H8HQ

- https://www.youtube.com/watch?v=UNXJG2jil3c - https://www.youtube.com/watch?v=_9ejrBQo8Kk - https://www.youtube.com/watch?v=wV0VB8XdlpM - https://www.youtube.com/watch?v=JoJoqts-PoQ - https://www.dailymotion.com/video/x2hifrq - https://www.youtube.com/watch?v=7Uip5WplSjQ - https://www.youtube.com/watch?v=um-X9Ea8Y_Y - https://www.youtube.com/watch?v=f3f0iHwjYtM - https://www.krackattacks.com/ - https://gbhackers.com/crack-wifi-network-passwords/

Wireless Hacking

- https://www.youtube.com/watch?v=1yaHe7zWg1k - https://rootsh3ll.com/rwsps-cracking-wps-with-reaver-pin-attack-ch3pt5/ - https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

- https://www.researchgate.net/publication/4339361_Beacon_Frame_Spoofing_Attack_Detection_in_IEEE_80211_Networks - https://medium.com/infosec-adventures/beacon-flooding-attack-a4baadc2242b - https://www.youtube.com/watch?v=PC7gaJNmo20 - https://medium.com/infosec-adventures/beacon-flooding-attack-a4baadc2242b - https://subscription.packtpub.com/book/networking_and_servers/9781785285561/8/ch08lvl1sec49/the-fake-beacon-flood-attack - https://kalilinuxtutorials.com/mdk3/ - https://www.youtube.com/watch?v=r1qsm0cqdhU - https://www.quora.com/Is-it-possible-to-hack-a-WPA-WiFi-by-just-spoofing-the-client-s-MAC-address

Wireless Hacking

- https://www.youtube.com/watch?v=cJ2JSU03D38 - https://www.youtube.com/watch?v=oQQhBdCQOTM - https://www.youtube.com/watch?v=aUY4LwByLeY - https://www.youtube.com/watch?v=C4GvfOR4Zik - https://www.youtube.com/watch?v=AbbYRYArucQ - https://www.youtube.com/watch?v=b5E0u4qNH4s - https://www.youtube.com/watch?v=olPlI9gEPUU - https://hacker-gadgets.com/blog/2019/09/17/top-20-hacking-gadgets/ - https://www.makeuseof.com/tag/how-to-make-a-wifi-antenna-out-of-a-pringles-can-nb/ - https://www.youtube.com/watch?v=KjGuqwMWMcA - https://www.youtube.com/watch?v=2te89R8SMoM - https://www.youtube.com/watch?v=Bkj3TBu0ZV4&list=PLW5y1tjAOzI0RhAkn_rWmq6iH0rRsWcHJ - https://github.com/search?q=wireless+hacking

Wireless Hacking

- https://www.youtube.com/watch?v=yehMWcCEq9I - https://www.youtube.com/watch?v=8kXbu2Htteg - https://www.youtube.com/watch?v=YDpjGTojByw - https://null-byte.wonderhowto.com/how-to/bluetooth-hacking/ - https://null-byte.wonderhowto.com/how-to/hack-bluetooth-part-1-terms-technologies-security-0163977/ - https://www.howtogeek.com/438712/could-your-bluetooth-devices-be-hacked-in-2019/ - https://www.insecure.in/bluetooth_hacking_02.asp- https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-hack-bluetooth-0163586/ - https://www.youtube.com/watch?v=xqTCmrdh3fs - https://www.youtube.com/watch?v=fS0pyv-Dz3c - https://null-byte.wonderhowto.com/how-to/bluetooth-hacking/by-hot/ - https://www.youtube.com/watch?v=lAtvGksBOiw - https://duo.com/decipher/bluetooth-hacking-tools-comparison - https://www.youtube.com/watch?v=SLLM7C7uMD4 - https://blog.attify.com/the-practical-guide-to-hacking-bluetooth-low-energy/ - https://hackersec.com/invasao-de-bluetooth-com-hardware/ https://null-byte.wonderhowto.com/how-to/bt-recon-snoop-bluetooth-devices-using-kali-linux-0165049/ -https://thehacktoday.com/hack-smartphone-bluetooth-using-kali-linux/ - https://subscription.packtpub.com/book/networking_and_servers/9781788995177/8/ch08lvl1sec71/bluetooth-hacking - https://github.com/search?q=bluetooth+hacking - https://www.linkedin.com/pulse/wireless-hacking-hands-on-al%C3%A9m-de-um-simples-brute-force-dos-santos/

Introdução ao Web App Hacking

Web Hacking

- https://owasp.org/www-project-top-ten/
- https://www.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://www.devmedia.com.br/sql-injection/6102
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A3-Sensitive_Data_Exposure
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A4-XML_External_Entities_(XXE)
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A5-Broken_Access_Control
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration

Web Hacking

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS)
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A8-Insecure_Deserialization
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities
- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A10-Insufficient_Logging%252526Monitoring
- https://pentest-tools.com/blog/xss-attacks-practical-scenarios/
- https://www.acunetix.com/websitesecurity/cross-site-scripting/
- https://portswigger.net/web-security/cross-site-scripting
- https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/
- https://portswigger.net/web-security/csrf
- https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/

Web Hacking

- https://www.solarwindsmsp.com/blog/remote-code-execution
- https://www.imperva.com/blog/remote-code-execution-rce-attacks-apache-struts/
- https://www.drizgroup.com/driz_group_blog/what-is-remote-code-execution-attack-how-to-prevent-this-type-of-cyberattack
- https://blog.hackmetrix.com/what-is-rce-remote-code-execution/

Introdução a Criptografia

Criptografia

- https://en.wikipedia.org/wiki/Hash_function
- https://www.cs.cmu.edu/~adamchik/15-121/lectures/Hashing/hashing.html
- https://mathworld.wolfram.com/HashFunction.html
- https://privacycanada.net/hash-functions/what-are-hash-functions/
- https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://searchsecurity.techtarget.com/definition/asymmetric-cryptography
- https://cryptography.io/en/latest/hazmat/primitives/asymmetric/
- https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
- https://aesencryption.net/
- https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard

Criptografia

- https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
- https://pt.wikipedia.org/wiki/Pretty_Good_Privacy
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://www.openpgp.org/
- https://en.wikipedia.org/wiki/RSA_(cryptosystem)
- https://www.cryptopp.com/wiki/RSA_Cryptography
- https://cryptography.io/en/latest/hazmat/primitives/asymmetric/rsa/
- https://whatismyipaddress.com/cryptography
- https://www.geeksforgeeks.org/digital-signatures-certificates/
- https://searchsecurity.techtarget.com/definition/digital-certificate

DUMPS PARA VOCÊ CONHECER A PROVA (Alguns são pagos, mas você pode achar gratuito em grupos de telegram de cupons de descontos dos cursos da Udemy):

https://www.udemy.com/course/certified-ethical-hacker-ceh-practice-exams/

https://www.udemy.com/course/ceh-v10-312-50-real-exam-tests-certified-ethical-hacker/

https://www.certification-questions.com/eccouncil-exam/ceh-dumps.html

https://www.prepaway.com/ceh-certification-exams.html

https://www.udemy.com/course/ceh-v10-exam-312-50-600-practice-exam-questions-dumps

FINISH