Marco Aurélio Thompson

técnicas que você precisa aprender para não ser um hacker idiota

A ESCOLA DE HACKERS APRESENTA:

APRENDA A SER HACKER PARA NÃO SER INVADIDO

como não ser um HACKER Idiota

www.escoladehackers.com

ISBN: 978-85-98941-71-4

DISTRIBUIÇÃO GRATUITA POR DOWNLOAD

Projeto gráfico, edição, revisão:

www.fb.com/marcoaureliothompson

Apresentação

O sucesso da coleção Aprenda a Ser Hacker para não ser Invadido – Série A com mais de 500 mil downloads até o começo de 2020, foi o que nos motivou a lançar a Série B com mais quatro e-books contendo importantes temas de estudo que interessam a quem é ou pretende ser hacker:

Aprenda a Ser Hacker para Não ser Invadido – Série A – Volume 1 a 6

A novidade da Série B é que os e-books são publicados pela Escola de Hackers[1] que volta a oferecer cursos, agora em parceria com a Udemy.

[1] www.escoladehackers.com

Os e-books da Série B são quatro e tratam dos seguintes assuntos:

1. o mínimo que você precisa **aprender** para não ser um hacker idiota
2. o mínimo que você precisa **ter** para não ser um hacker idiota
3. **técnicas** que você precisa aprender para não ser um hacker idiota
4. **softwares** que você precisa aprender para não ser um hacker idiota

Aprenda a Ser Hacker para Não ser Invadido – Série B – Volume 7 a 10

Os e-books procuram responder as perguntas mais comuns formuladas pelos iniciantes nos grupos e nas redes sociais. Estas perguntas parecem estúpidas e ingênuas, mas escondem uma intenção real no aprendizado e geralmente são mal respondidas, as respostas são incompletas ou quem pergunta é recebido com ofensas, tornam-se vítimas de ataques ou são tratadas com desdém.

Esperamos que os e-books da Escola de Hackers possam mudar isso e contribuam com respostas simples, completas e embasadas em nossos mais de trinta anos na profissão. Já somos a maior, queremos ser a melhor também. E começamos respondendo a primeira pergunta do iniciante, que é:

O que preciso **aprender** para ser hacker?

A resposta está no e-book:

A propósito, a palavra idiota está sendo usada como sinônimo de lamer (ou lammer) e também para pegar carona na onda de livros que estão usando esta palavra na capa e vendendo bem. 😉

> Segundo o Jargon File[2] lamer é alguém com pouco conhecimento hacker que se revela ao fazer perguntas idiotas em grupos e fóruns. Uma pergunta típica de lamer é justamente sobre o que precisa aprender para ser hacker, temas dos nossos e-books.

Outra pergunta comum feita pelo iniciante, é:

> O que preciso **ter** para ser hacker?

A resposta está no e-book:

> O mínimo que você precisa **ter** para não ser um hacker idiota

O *ter* pode representar várias coisas: equipamento, conexão, softwares, conhecimento, etc. Em nosso e-book tratamos de tudo isso e também analisamos o artigo Como se Tornar um Hacker do Eric S. Raymond[3].

[2] http://catb.org/jargon/html/L/lamer.html
[3] https://www.linux.ime.usp.br/~rcaetano/docs/hacker-howto-pt.html

Outra pergunta comum feita pelos iniciantes diz respeito as técnicas hacker. Para ajuda-los com isso reunimos todas as técnicas que encontramos, o que dá um total de quase 400 técnicas no e-book. É um compêndio de técnicas tão completo que vai interessar até a quem não é iniciante:

Iniciantes também vivem perguntando sobre ferramentas hacker e de segurança. As perguntas costumam ser:

> Qual o melhor programa para invadir e-mail?
> Qual o melhor programa para invadir contas do Facebook?
> Qual o melhor programa para invadir redes sem fio?

A resposta está no e-book:

A propósito, estes e-books não substituem e nem são cursos de invasão. O objetivo desses e-books é orientar o iniciante em suas dúvidas mais comuns,

porém não se trata de e-books com cursos ou tutoriais. Os e-books mostram os possíveis caminhos, mas quem tem que escolher um e percorrê-lo é você.

Da mesma forma que ao ser respondido em algum fórum ou grupos ninguém vai te dar aula particular, nossos e-books são informativos, não são cursos e nem foram escritos com este propósito.

Se você procura por livros e e-books que ensinem pentest ou invasão para testar a segurança, informe-se sobre nossas publicações que podem ser vistas no Skoob[4], Issuu[5], Clube de Autores[6] ou na Udemy[7].

Agora, se tudo o que você quer são respostas para as perguntas mais comuns feitas por quem está começando, então, está no lugar certo.

Boa leitura! 😊

[4] https://www.skoob.com.br/autor/livros/12924
[5] https://www.issuu.com/editoradoautor
[6] www.clubedeautores.com.br
[7] www.udemy.com/user/escola-de-hackers

Técnicas que você precisa **aprender** para não ser um hacker idiota

Meu primeiro computador foi um TK-85 comprado em 1984 quando ainda era adolescente. Foi preciso juntar meu primeiro salário com uma ajudinha do pai.

No mesmo ano fiz precisei fazer uma série de modificações no aparelho, o que já poderia dar-me o título de hacker, porque nessa época hacker era quem fazia modificações no hardware quando poucos eram capazes de fazer isso.

Para não ficar muito forçado prefiro usar como data da minha *titulação* o ano de 1987, quando iniciei como phreaker (hacker de telefonia) e criei o diodo Thompson. E assim se passaram 33 anos sem eu nunca ter tirado os dedos de um teclado de computador ou deixado de procurar formas de *hackear*.

Os computadores para mim sempre foram limitados ou impunham alguma restrição. Quando não eram restrições financeiras ou limitações relacionadas ao desempenho, eram restrições relacionadas ao acesso.

Como exemplo de restrição financeira, posso citar a conta telefônica no tempo em que acessávamos BBS e depois a internet usando conexão discada. Antes de eu cuidar disso *a moda hacker*, minha conta chegou a quase 800 reais em um único mês.

Como exemplo de limitações relacionadas ao desempenho, posso citar a dificuldade que era rodar jogos no tempo do MS-DOS ou do Windows 3.1. Era preciso gerenciar a memória, fazer modificações nos arquivos autoexec.bat e config.sys e bastava ter que instalar um novo periférico para nos vermos às voltas com a BIOS e jumpers de configuração de endereço IRQ e DMA.

Pensando bem, acho que não dava para não ser hacker na década de 1980, de tanta coisa que você precisa mexer por fora se quisesse fazer um computador funcionar do seu jeito.

Os últimos obstáculos que encontrei foram as restrições relacionadas ao acesso. Esse tipo é o que me acompanha até hoje e está mais próximo das limitações que você vai ter.

Tudo começou com a limitação de tempo de acesso. Antes da internet usávamos um sistema local conhecido como BBS[8], que pode ser traduzido como Quadro de Avisos Eletrônico.

No BBS você participava de fóruns, enviava e recebia e-mails, baixava programas, fazia algumas consultas a serviços públicos.

A internet ainda era restrita a governos, universidades e centros de pesquisa, mas dava para acessar alguma coisa a partir do BBS.

Era um mundo novo e — pelo menos para mim — o acesso ao BBS era muito viciante, mas limitado a uma hora por dia. Foi esta necessidade de ter mais tempo de acesso que me fez procurar formas de acessar por mais tempo, o que foi conseguido com a técnica *password guessing*, que funciona até hoje.

Foi invadindo contas de usuários que consegui mais tempo de acesso, até descobrir como criar minha conta de SysOp (operador do sistema).

Quando a internet foi liberada no final de 1994 foi feito um sorteio pela Embratel, uma Estatal que detinha o monopólio do acesso comercial à internet no Brasil. Não foi um dos sorteados, porém, mais uma vez o *password guessing* me salvou.

[8] Bulletin Board System

Tornei-me hacker por força do acaso e nunca imaginei que viveria disso. Havia necessidades que precisavam ser satisfeitas, havia restrições e limitações que precisavam ser superadas e tudo o que fiz foi procurar formas de fazer o sistema submeter-se a mim e satisfazer minhas necessidades pontuais; é assim até hoje.

Acredito que o seu caso seja exatamente o mesmo que me levou a ser hacker. Você deve estar insatisfeito com as restrições e limitações relacionadas a desempenho, financeiras ou acesso e já entendeu que só o conhecimento hacker será capaz de resolver isso. Resolver para você e para outros que estejam passando pelo mesmo problema e que poderão contar com você para resolver a situação.

Se este é o caso me deixa te contar um segredo. Quem vai resolver isso para você é a técnica. Não é o melhor computador, não é um monte de cursos e livros, não é a melhor ferramenta e nem o Linux Kali. O segredo de todo hacker é a técnica. Saber quais existem e qual é a mais indicada para cada problema (restrição ou limitação) que ele vai encontrar.

Se você quer ser um hacker de verdade preocupe-se em aprender técnicas. Comece pelas mais fáceis, depois aprenda as principais e mais adiante dedique-se as técnicas novas ou pouco conhecidas. Só a técnica é capaz de proporcionar uma ação hacker.

O software ou ferramenta de segurança é acessório da técnica. Para a técnica qualquer programa e qualquer sistema operacional serve. Da mesma forma, saber programar ou usar um sistema operacional próprio para hackear, tudo está a serviço da técnica. Dominando a técnica você decide qual ferramenta e qual sistema operacional quer usar. Torna-se livre, sem limitações.

No e-book de hoje reunimos quase quatrocentas técnicas listadas alfabeticamente e para você entender a importância deste material, pense no seguinte:

1. Não há em toda a internet uma lista tão completa reunindo praticamente todas as técnicas hacker que existem, desde as mais antigas até as atuais;
2. Se você leu nosso outro e-book, **o mínimo que você precisa aprender para não ser um hacker idiota**, já sabe que um dos conhecimentos necessários é o conhecimento das técnicas hacker. Se havia dúvidas de quantas e quais seriam estas técnicas, com este e-book essa dúvida não existe mais;
3. Ser hacker é saber selecionar alvos, identificar a vulnerabilidade e usar a técnica, mas tem que ser a técnica adequada para o tipo de alvo. Quem se diz hacker e não sabe selecionar alvos ou não conhece as técnicas pode fazer quantos cursos quiser e nunca será hacker; não terá resultado em suas ações;
4. Um bom hacker é aquele que domina boas técnicas;
5. Para terminar, toda ação hacker é obtida com o uso das técnicas.

A propósito, você está recebendo a primeira versão deste e-book. Diferentemente dos outros que são repletos de informações, nesta primeira versão você só vai ter a lista das técnicas e nada mais.

A boa notícia é que após a relação das técnicas você fica sabendo o que estamos preparando para a segunda edição, bem como um link para cadastrar seu e-mail e ser informado(a) assim que lançar.

Lista em Ordem Alfabética de (quase) Todas as Técnicas Hacker Conhecidas no Mundo[9]

1. 0Day
2. 802.1q Double Tagging
3. Account Lockout
4. AI-powered Attack
5. Anonymity
6. Application-based Denial of Service
7. APT (Advanced Persistent Threats)
8. ARP Poisoning - ARP (Address Resolution Protocol) Attack
9. ARP Redirect - ARP (Address Resolution Protocol) Attack
10. ARP Spoofing - ARP (Address Resolution Protocol) Attack
11. Asymmetric Resource Consumption (Amplification)
12. ATM Hacking
13. Attacking Authentication
14. Backdoor
15. Badge Surveillance
16. Baiting (Social Engineering)
17. BCS (Badly Configured System)
18. BEAST (Browser Exploit Against SSL/TLS) Attack (TLS/SSL Vulnerabilities)
19. BEC (Business Email Compromise)

[9] Se você conhece alguma técnica que não esteja na lista, por favor nos avise entrando em contato conosco.

20. Binary Planting
21. Birthday Attack
22. Bitcoin Race Attack
23. Blind XPath Injection
24. Blue Jacking - Blue Spamming
25. Bluebugging
26. Bluesnarfing
27. BotNet - RoBOT NETwork - Zombie Network
28. Bots
29. Bounds Check Bypass
30. Branch Target Injection
31. BREACH Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext Attack (TLS/SSL Vulnerabilities)
32. Browser Hijacker
33. Browser Modifier
34. Brute Force
35. Brute-force HTTP Flood Attacks
36. Burp Intruder Attack
37. Cache Attack
38. Cache Poisoning
39. CAM (Content Addressable Memory) Table Overflows
40. CAM Table Overflow
41. Carding (fraud)
42. Casemod (Hardware Hacking)
43. Cash Overflow
44. CDN (Content Delivery Network) Proxy Attack

45. Clickjacking - Clickjack Attack
46. Cloning
47. CMS Attack (WordPress, Joomla, Magento, Moodle, etc.)
48. Code Injection
49. Command Injection
50. Comment Injection Attack
51. Content Spoofing
52. Cookie Theft
53. CORS Origin Header Scrutiny
54. CORS Request Prefligh Scrutiny
55. Credential Reuse Attack
56. Credential Stuffing
57. CRIME (Compression Ratio Info-leak Made Easy) Attack (TLS/SSL Vulnerabilities)
58. Cross Frame Scripting
59. Cross User Defacement
60. Cryptanalysis
61. Cryptojacking
62. CSFR (Cross Site Forgery Request)
63. CSRF (Cross Site Request Forgery) - XSRF
64. CSV (Comma Separated Values) Injection
65. Custom Special Character Injection
66. Cyber-Physical Attack
67. Cybersquatting
68. DAI (Dynamic ARP Inspector)
69. Data Breaches

70. Data Recovery Attack
71. Data Scraping
72. Data Theft
73. DDoS (Distributed Denial of Service)
74. DHCP (Dynamic Host Configuration Protocol) Snooping
75. DHCP (Dynamic Host Configuration Protocol) Spoofing
76. Dictionary Attack
77. Direct Dynamic Code Evaluation - Eval Injection
78. Direct IP Attack
79. Directory Harvest Attack
80. Directory Listing
81. Directory Traversal - Path Traversal
82. DLL (Dynamic-Link Library) Load Order Hijacking
83. DNS (Domain Name System) Poisoning
84. DNS (Domain Name System) Spoofing
85. DNS (Domain Name System) Tunneling
86. DoS (Denial of Service)
87. Dos/DDoS - Aplicação (HTTP Flood)
88. DoS/DDoS - Protocolo (SYN Flood, Ping of Death, Smurf, LAND)
89. DoS/DDoS - Volumétrico (TCP Flood, ICMP Flood)
90. Double Encoding
91. Doxing - Doxxing
92. Drive-by Attack - Drive-by Download Attack
93. DROWN (TLS/SSL Vulnerabilities)
94. Dumpster Diving
95. EAR (Execution After Redirect)

96. Eavesdropping Attack
97. Electronic Badge Authentication
98. Electronic Pickpocketing (Hardware Hacking)
99. Email Fraud
100. Engenharia Social
101. Enumeration
102. Esteganografia
103. Evil Twin Attack
104. Exploitation - Exploiting
105. Exploiting a Back Door
106. Fake ID
107. Fake News Attack
108. Fiber Tapping
109. Fingerprint
110. Flood
111. Footprint
112. Forced Browsing
113. Form Action Hijacking
114. Format String Attack
115. Formula Injection - Spreadsheet Formula Injection
116. FPD (Full Path Disclosure)
117. Fraggle Attac
118. FUD (Fully UnDetectable)
119. Function Injection
120. Google Hacking
121. Gray-Mail

122. HackRF On Attack
123. Hardware Keylogger Attack (AirDrive, KeyGrabber, SerialGhost, MorphStick, VideoGhost)
124. HEARTBLEED (TLS/SSL Vulnerabilities)
125. Hijacking
126. Hoax
127. Host Header Injection
128. HTTP Flood
129. HTTP Request Smuggling
130. HTTP Response Splitting
131. HTTP Tunnel (Reverse Shell Attack)
132. HTTPS Spoofing
133. ICMP Redirect
134. ICMP Tunneling
135. ICMP Unreachable
136. ID Theft - Identity Theft
137. Identity Cloning
138. Idle scan
139. iFrame Injection
140. Ijacking (Identity hiJACKING)
141. Inference attack
142. InfoCC
143. Injeção de Script
144. Injeção de SQL
145. Input/Output Patching - I/O Patching (Hardware Hacking)
146. Insider Attack

147. Insider Threats
148. IP Address Spoofing
149. IP Source Guard
150. IP Spoofing
151. IRDP (ICMP Router Discovery Protocol) Spoofing
152. JTAG/UART - Hex Dumping (Hardware Hacking)
153. Kerberoasting (Kerberos AD Attack)
154. Kiosk Hacking
155. L1TF (L1 Terminal Fault)
156. LAN Turtle Attack
157. LAND (Local Area Network Denial) Attack
158. Lazy FPU - Lazy FP State Restore - Lazy FPU State Leak - LazyFP
159. LDAP Injection
160. LDAP Reconnaissance (PowerSploit and PowerShell) - AD Attack
161. LFI (Local File Inclusion) Attack
162. Local Admin Mapping (Bloodhound) - AD Attack
163. Lock Bumping
164. Lock Picking
165. Log Injection
166. Logic Analyzer (Hardware Hacking)
167. Looping User Datagram Protocol (UDP) Ports
168. Lottery Scam
169. Low Tech Attack - No Tech Attack
170. MAC (Media Access Control) Spoofing
171. Malware - Adware
172. Malware - Cookies On-Off

173. Malware - Hijackware
174. Malware - Keystroke logging – Keylogger
175. Malware - Lampion
176. Malware - Logic Bomb
177. Malware - Macro Viruses
178. Malware - MALicious softWARE
179. Malware - Nagware, Begware, Annoyware, Nagscreen
180. Malware - PUA (Potentially Unwanted Program) - PUP (Potentially Unwanted Program) - PPI (Programa Potencialmente Indesejável)
181. Malware - Ransomware
182. Malware - Scareware
183. Malware - Screenlogger
184. Malware - Scumware
185. Malware - Spyware
186. Malware - Time Bomb
187. Malware - Viruses
188. Malware - Worms
189. Management Interface Exploits
190. Man-in-the-browser
191. Man-in-the-middle (MitM) attacks - once malware has breached a device
192. Man-in-the-middle (MitM) attacks - proxye
193. Man-in-the-middle (MitM) attacks - unsecure public Wi-Fi
194. Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
195. Microarchitectural Fill Buffer Data Sampling (MFBDS)
196. Microarchitectural Load Port Data Sampling (MLPDS)

197. Microarchitectural Store Buffer Data Sampling (MSBDS)
198. Misconfigurations
199. Mixed Threat Attack
200. Mobile Code Invoking Untrusted Mobile Code
201. Mobile Code Non-final Public Field
202. Mobile Code Object Hijack
203. Modified Operating System Attack
204. Network of Living Zombies
205. NTDS.dit Extraction (VSSAdmin, PowerSploit, and Hashcat) - AD Attack
206. OS Command Injection attack
207. Overclocking (Hardware Hacking)
208. Overflow Vulnerabilities - Buffer Overflow (Binary Exploitation) (Buffer Overflow with Environment Variables)
209. Overflow Vulnerabilities - Heap Overflow
210. Overflow Vulnerabilities - Stack Overflow
211. P2P Hacking
212. Page hijacking
213. Parameter Delimiter
214. Parameter Tampering
215. Password Attack - Brute-force
216. Password Attack - Dictionary attack
217. Password attacks - Keylogger attacks
218. Password attacks - Password Cracking - Bruteforce Attacks
219. Password attacks - Password Cracking - Dictionay Attacks
220. Password attacks - Password Guessing

221. Password attacks - Password sniffing
222. Password Sniffing - Password Stealer
223. PayPal
224. People Watching
225. Perimeter Network Vulnerabilities
226. Pharming
227. Phishing - Scam
228. Phishing - Smishing (SMS phishing)
229. Phishing - Spear phishing
230. Phishing - Vishing (Voice phishing)
231. Phishing - Whaling ou Whale Phishing
232. Phone cloning
233. Phone Tapping
234. Phones Recording
235. PHP Injection
236. Piggybacking
237. Ping flood
238. POD (Ping of Death)
239. POODLE (Padding Oracle On Downgraded Legacy Encryption) Attack (TLS/SSL Vulnerabilities)
240. POR (Relative Path Overwrite)
241. Port Scanning
242. Port Stealing
243. Preimage Attack
244. Pretexting
245. Privileged Account Management

246. Pwned Attack
247. QRLJacking - Quick Response Code Login Jacking
248. Quid Pro Quo
249. Race Condition Attack
250. Rainbow Table Attack
251. RCE (Remote Code Execution)
252. ReDoS - Regular expression Denial of Service
253. Reflected DOM Injection
254. Remote Recording
255. Replacing a Component (Hardware Hacking)
256. Repudiation Attack
257. Resource Injection
258. Reverse Engineering
259. Reverse Tabnabbing
260. Reverse RDP Attack
261. RFI (Remote File Inclusion) Attack
262. RFID Attack
263. Rogue Data Cache Load
264. Rogue System Registry Read - Meltdown Attack
265. Rogue Wireless Devices
266. Rootkit
267. Route Mangling
268. Scam Baiting
269. Session Fixation
270. Session Hijacking
271. Session Prediction

272. Setting Manipulation
273. Sextortion Attack
274. Shoulder Surfing
275. SIM Swap
276. SMB Relay
277. Smurf Attack
278. Sniffing
279. Software Cracking
280. Software Theft
281. Source Code Disclosure
282. Spam
283. Special Element Injection
284. Spoofing - Address Bar Spoofing
285. Spoofing - eMail spoofing
286. Spoofing - IP spoofing
287. SQL Injection (SQLi) - In-band SQLi (Classic SQLi) - Error-based SQLi
288. SQL Injection (SQLi) - In-band SQLi (Classic SQLi) - Union-based SQLi
289. SQL Injection (SQLi) - Inferential SQLi (Blind SQLi) - Boolean-based (content-based) Blind SQLi
290. SQL Injection (SQLi) - Inferential SQLi (Blind SQLi) - Time-based Blind SQLi
291. SQL Injection (SQLi) - Out-of-band SQLi
292. SSB (Speculative Store Bypass) - Spectre Attack
293. SSI (Server-Side Includes) Injection
294. SSL-based DDoS Attack

295. SSRF (Server Side Request Forgery)
296. Stalking
297. Stealing Passwords from Memory (Mimikatz) - AD Attack
298. STP (Spanning-Tree Protocol) Mangling
299. SWAPGS — Swap GS Base Register Attack
300. Switch Spoofing
301. SYN Attack
302. Tailgating
303. Tampering
304. TCP Flood
305. TCP Sesynchronization
306. TCP Sequence Prediction Attack
307. Teardrop
308. Traffic flood
309. Traffic Tunneling Attack
310. Trojan Backdoor
311. Trojan Banker
312. Trojan Clicker
313. Trojan Destrutivo
314. Trojan DoS
315. Trojan Downloader
316. Trojan Dropper
317. Trojan Horse (Cavalo de Troia)
318. Trojan Proxy
319. Trojan Spy
320. Trolling

321. Ubertooth One Attack
322. UDP Flood
323. UDP Reflectors
324. Unicode Encoding
325. URL Attack - HTTP bombing
326. URL Interpretation
327. USB Rubber Ducky Attack
328. Van Eck phreaking
329. Vehicle Surveillance
330. VLAN (Virtual LAN) Hopping Attack
331. VPN (Virtual Private Network) Attack - Generic Routing Encapsulation (GRE) - IP in IP tunnel (IPIP) Packets
332. Vulnerable JavaScript Libraries
333. War Dialing
334. War dialing
335. Warchalking
336. Wardriving
337. Warez
338. Watering Hole Attack
339. Wayback Machine Attack
340. Weak Password
341. Web Management Interfaces
342. Web Parameter Tampering
343. Web Skimming
344. Webtapping
345. WiFi eavesdropping

346. WiFi Pineapple Attack
347. Windows ::DATA Alternate Data Stream
348. Wireless Hijacking
349. Wiretapping
350. WPS (WiFi Protected Setup) Attack
351. X-by-Ware Attack
352. XFS (Cross Frame Scripting)
353. XPATH Injection
354. XSHM (Cross Site History Manipulation)
355. XSS (Cross Site Scripting) Attack - DOM-based XSS - Server XSS - Client XSS
356. XSS (Cross Site Scripting) Attack - Reflected (Persistent) XSS
357. XSS (Cross Site Scripting) Attack - Stored (Persistent) XSS
358. XSS (Cross Site Scripting) in Subtitle Attack
359. XST (Cross Site Tracing)
360. XXE (XML External Entity) Attack
361. Zero-day Attack
362. Zero-day Exploit

Sobre a primeira versão deste e-book

A primeira versão deste e-book, que é esta, certamente vai te surpreender pela grande quantidade de técnicas reunidas, mas vai ser também uma grande frustração, porque limitamo-nos a listar as técnicas. Explicações mais completas vêm depois, conforme o número de downloads da primeira versão.

Digo isto porque estou me colocando no seu lugar e o que eu gostaria de ver é uma descrição completa da técnica, com exemplo de uso, links para saber mais e até videoaulas explicando algumas, se der.

Tudo isso está previsto, mas não para esta primeira versão. Hoje o que temos para você é apenas a lista de todas as técnicas conhecidas, desde as mais antigas até as mais atuais e se você sentir falta de alguma é só enviar para o nosso e-mail que ele vai estar presente na próxima atualização.

Enquanto você toma conhecimento de todas as técnicas hacker que existem, entende a importância de conhecer um punhado delas e faz uma autoavaliação para ver quais conhece e quais ainda falta conhecer, nos bastidores estaremos trabalhando na atualização deste material.

A próxima versão deste e-book vai incluir uma divisão das técnicas por categoria e cada técnica terá uma ficha completa, mais ou menos assim:

Nome da técnica: geralmente o título pelo qual a técnica é conhecida em inglês e a tradução.
Categoria: categoria a qual a técnica pertence.
Onde usar: alvo indicado para o uso da técnica.
O que precisa para usar a técnica: descrição do hardware, plataforma, software, script; na verdade um checklist do que é necessário para executar a técnica.

Descrição da técnica: como é a técnica, quando surgiu, breve descrição do funcionamento.
Tecnologia relacionada: tecnologia relacionada à técnica.
Exemplo de uso: estudo de caso com análise de casos reais em que a técnica foi usada.
Como usar: é o como fazer, o tutorial ilustrado com as telas de cada etapa incluindo um fluxograma passo a passo para orientar.
Para saber mais: links e livros que tratam da técnica e podem ser baixados ou consultados na internet.
Videoaula: explicando e demonstrando a maioria ou pelo menos as técnicas mais usadas e de maior alcance.
Arquivos: todo o material necessário para a execução da técnica, podendo incluir scripts, exploits, softwares, máquinas virtuais pré-configuradas, metasploitables, etc.

Para ser avisado quando a versão mais completa deste e-book estiver pronta, faça o seu cadastro gratuito em:

www.escoladehackers.com/tecnicas

Quem é esse cara?

Marco Aurélio Thompson é um dos dez maiores hackers brasileiros, com registro de atividade desde 1987 como phreaker (hacker de telefone).

Em 2003 lançou o Curso de Hacker[1] e em 2007 a Escola de Hackers[2], pois sempre acreditou que a melhor defesa contra hackers é se tornar um, isto em uma época em que hackers não eram vistos com bons olhos.

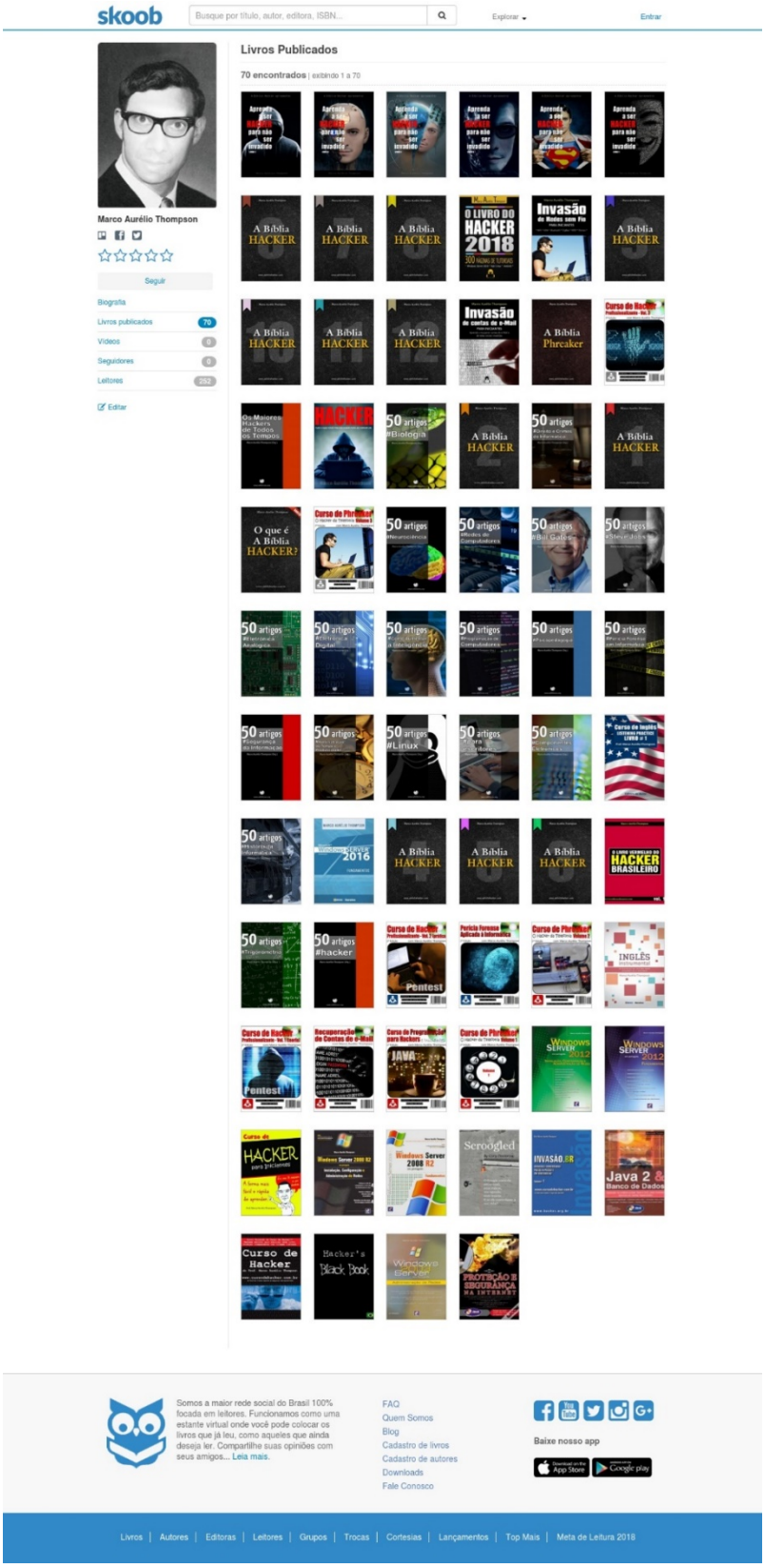
É professor, empresário, jornalista, consultor pelo Sebrae e de uns tempos para cá passou a colecionar diplomas universitários:

- MBA em Gestão de TI pela FMU
- Bacharel em Sistemas de Informação pela Unifacs
- Bacharel em Administração de Empresas pela Unifacs
- Pedagogo pela Unifacs
- Pós-graduado em Psicopedagogia pela Unifacs
- Pós-graduado em Ethical Hacking e CyberSecurity pela Uniciv
- Pós-graduando em Forense Computacional pela Uniciv
- Licenciado em Letras pela Unifacs
- Licenciando em História pela Estácio
- Licenciando em Matemática pela Estácio
- Estudante de Direito na Universidade Federal da Bahia (UFBA)
- Em andamento um projeto de Mestrado em Educação

Lista atualizada até 2020, depois disto já deve ter mais alguma coisa. 😉

[1] www.cursodehacker.com.br | www.cursodehacker.com
[2] www.escoladehackers.com.br | www.escoladehackers.com

O maior autor hacker do mundo



Fonte: www.skoob.com.br/autor/livros/12924

Fale Conosco

E-Mail

Não use[3].

Site

http://www.MarcoAurelioThompson.com

Youtube

www.youtube.com/marcoaureliothompson

Udemy

www.udemy.com/user/marco-aurelio-thompson

Facebook

www.fb.com/marcoaureliothompson

WhatsApp

+55 (71) 9-9130-5874

LinkedIn

www.linkedin.com/in/marcoaureliothompson

Currículo Lattes

www.marcoaurelio.net/currículo

Instagram

www.instagram.com/marcoaureliothompson

[3] A forma menos recomendável para entrar em contato conosco é por e-mail. Devido a palavra *hacker* a maioria dos provedores bloqueia as mensagens por conta do conteúdo ou do remetente. Dê preferência ao Facebook ou WhatsApp.