

The background is a gradient of deep purple and blue, speckled with small white dots. On the left side, there are several concentric circular patterns and a large arc with a scale. The scale has numbers ranging from 140 to 260 in increments of 10. There are also smaller circular elements with arrows indicating direction.

TAKING A GIAC EXAM

KEVIN TYERS

INSPIRATION



- <https://tisiphone.net/2015/08/18/giac-testing/>

BASICS

- 1 proctored exam
- 100-150 questions
- Time limit of 4 hours
- Minimum Passing Score of 73%
- Open Book (Arm Full of Books)
- No electronics (including Apple Watch probably)

COMMON PROBLEMS

- Cramming in the last month
- Ignoring your Labs
- Ignoring your MP3s

- Your Index is your best tool!
- Topic – Page – Book – Notes
- Consistent Topics
 - I like “Noun” based topics

- 3.150 Command Shell workarounds for Linux
- 3.138 Command Shell workarounds for Windows
- 1.35 Commercial Tools
- 1.131 Competitive Intelligence / OSINT
- 5.56 CoWPAtty - WPA dictionary attacks
- 3.175 credump - cached auth credential exfil
- 5.109 CSRF / XSRF
- 4.122 CUDA based GPU Password Cracking
- 4.35 Dictionary Generator (Fonlow)
- 4.121 Djohn, John-MPI, Dnet)
- 1.166 DNS - Cache Snooping
- 1.163 DNS - Record Types
- 1.165 DNS - Zone Transfers
- 1.120 Dradis
- 2.170 enum
- 2.166 Enumeration - Account Names
- 2.171 Enumeration - Enumerating SIDs
- 2.167 Enumeration - Harvesting E-Mail Addresses
- 2.168 Enumeration - Windows and Linux Users
- 2.167 eSearchy
- 1.10 Ethical Hacking - Definition
- 1.141 Exittool
- 1.8 Exploit - Definition
- 3.4 Exploitation - Definition
- 3.8 Exploits - Categories (service client, privesc)
- 3.10 Exploits - Client Side
- 3.17 Exploits - Local Privilege Escalation
- 4.83 fgdump
- 1.42 Firewall / NAT Concerns with Pen Testing
- 1.33 Free Tools and Exploits
- 1.178 FSDB, SLDB - Competitors to GHDB
- 1.133 Gloadin - Google Cache Searcher
- 1.176 Google Dork, GHDB, Examples
- 1.175 Google Hacking - ext, filetype
- 1.174 Google Hacking - intitle, inurl
- 1.173 Google Hacking - site, link
- 1.133 gpscan.rb - OSINT tool
- 1.38 Hardware for Pen Testing
- 4.123 Hashcat and oclHashcat (Hybrid GPU/CPU)
- 1.29 Infrastructure for Ethical Hacking
- 5.35 InSSiDer
- 5.129 Jikto - XSS Nikto Scanner
- 4.114 John The Ripper
- 4.116 John The Ripper - john.pot / john.rec recovery
- 5.73 Karma - WAP Impersonation

MP3S

- From a different class/get different perspective
- Tip: Make into Podcast, and listen as fast as you can and still understand (1.25-2x speed)
- Great for a commute or exercise

PRACTICE TESTS

- Very Realistic
- Don't Google!!!!
- Take first after you finish the content (1 or 2 passes)
- Take second like a real test

QUESTIONS

- Read Answers
- Read Question
- Eliminate Bad Answers
- Answer

QUESTION EXAMPLE

- **The Hobby that Kevin loves that will extend his life**
- A) Playing the Banjo
- B) Brazilian Jiu Jitsu
- C) Knitting
- D) Mechanical Keyboards

PRACTICALS

- A fair challenge
- Get good with your lab material
- At the end of the test

KEVIN'S DETAILED STUDY PLAN ~3 MONTHS

- Take Class – 1 Week
- Break – 1 Week
- Read Books/Do Labs – 2 Weeks
- Listen to Mp3s – 2 Weeks
- Practice Test 1
- Index Books/Do Labs – 2 Weeks
- Listen to Mp3s – 2 Weeks
- Deep Study on Weak Topics – 2 Weeks
- Practice Test 2
- Actual Test



QUESTIONS?