

# How to Prepare for the Certified Ethical Hacker Exam



Dale Meredith

@dalemeredith | [www.dalemeredith.com](http://www.dalemeredith.com)

“

If it wasn't "hard", everyone would do it...  
"hard" is what makes "it" great.

— Tom Hanks (League of their Own)

”

# Learn It, Love It, Live It



- ❑ About the Exam
- ❑ How to Prepare
- ❑ The SuperDale Method
- ❑ When in Doubt

---

# About the Exam

---

# 312-50 Exam Overview

125 questions  
Multiple choice

4 hours  
2 min. per question

70% to pass  
Prometric/VUE

---

# How to Prepare

---

# Requirements

2 years security  
experience

Education reflects  
background in  
Information Security

Remit \$100 eligibility  
application fee

# Requirements

Submit exam  
eligibility application

Purchase exam  
voucher from EC-C

Schedule exam  
(\$500)



# Study

Understanding of all  
19 domains

SQL injection & port  
scanning

Know your tools

# “Master of My Domain”

- 1) Intro to Ethical Hacking
- 2) Foot Printing/Reconnaissance
- 3) Scanning Networks
- 4) Enumeration
- 5) System Hacking
- 6) Trojans & Backdoors
- 7) Viruses & Worms
- 8) Sniffers
- 9) Social Engineering
- 10) Denial of Service

# “Master of My Domain”

- 11) Session Hijacking
- 12) Hacking Webservers
- 13) Hacking Web Applications
- 14) SQL Injection
- 15) Hacking Wireless Networks
- 16) Evading IDS, Firewalls, & Honeypots
- 17) Buffer Overflows
- 18) Cryptography
- 19) Penetration Testing

# Exam “Weight”

Section	Knowledge of	Weight	# of ?
Background	Networking technologies (e.g., hardware, infrastructure)	4%	5
	Web technologies		
	Systems technologies		
	Communication protocols		
	Malware operations		
	Mobile technologies		
	Telecommunication technologies		
	Backups and archiving		

# Exam "Weight"

Section	Knowledge of	Weight	# of ?
Analysis/Assessment	data analysis	13%	16
	systems analysis		
	risk assessments		
	technical assessment methods		

# Exam "Weight"

Section	Knowledge of	Weight	# of ?
Security	systems security controls	25%	31
	application/fileserver		
	firewalls		
	cryptography		
	network security		
	physical security		
	threat modeling		
	verification procedures		

# Exam “Weight”

Section	Knowledge of	Weight	# of ?
Security	social engineering	25%	31
	vulnerability scanners		
	security policy implications		
	privacy/confidentiality (regarding engagements)		
	biometrics		
	wireless access technology		
	trusted networks		
	vulnerabilities		

# Exam “Weight”

Section	Knowledge of	Weight	# of ?
Tools/Systems	network/host based intrusion	32%	40
	network/wireless sniffers		
	access control mechanisms		
	cryptography techniques		
	programming languages		
	scripting languages		
	boundary protection appliances		
	network topologies		



# Exam “Weight”

Section	Knowledge of	Weight	# of ?
Tools/Systems	subnetting	32%	40
	port scanning		
	domain name system		
	routers/modems/switches		
	vulnerability scanner		
	vulnerability management and protection systems		
	operating environments		
	antivirus systems and programs		

# Exam "Weight"

Section	Knowledge of	Weight	# of ?
Tools/Systems	log analysis tools	32%	40
	security models		
	exploitation tools		
	database structures		

# Exam “Weight”

Section	Knowledge of	Weight	# of ?
Procedures &	cryptography	20%	25
Methodology	public key infrastructure		
	Security Architecture		
	Service Oriented Architecture		
	information security incident management		
	N-tier application design		
	TCP/IP networking (e.g., network routing)		
	security testing methodology		

# Exam "Weight"

Section	Knowledge of	Weight	# of ?
Regulation/Policy	Security policies	4%	5
	Compliance regulations		

# Exam "Weight"

Section	Knowledge of	Weight	# of ?
Ethics	Professional code of conduct	2%	3
	Appropriateness of hacking activities		

---

# The SuperDale Method

---

# SuperDale's Method

- ❑ Multiple choice
- ❑ Select all that apply
- ❑ Read the answers 1<sup>st</sup>
- ❑ Understand each answer
- ❑ Read the questions backwards

- 1) If you've been contracted to perform an attack against a target system, what type of hacker are you?
  - a) White Hat?
  - b) Gray Hat?
  - c) Black Hat?
  - d) Red Hat?

---

When in Doubt...

---



# Who Wants to be a Millionaire?


- ❑ 50/50 Rule
  - ❑ Eliminate that which is false
  - ❑ Sherlock Holmes
- 1) What is a self-replicating piece of malware?
    - a) A Worm
    - b) A Virus
    - c) A Rootkit
    - d) A Trojan Horse

by Dale Meredith

## Discussion

0 comments

livefyre

 SuperDale

1 person listening




   + Follow

 Share

**Post comment**


Newest | Oldest | Top Comments


### Course content

 Table of contents

 Description

 Transcript

 Exercise files

 Assessment

 **Discussion**

### More info

Level **Beginner**

Rating 

Duration **3h 42m**

Released **19 Dec 2014**

# Summary



- ❑ About the Exam
- ❑ How to Prepare
- ❑ The SuperDale Method
- ❑ When in Doubt