CEH™ v12

CERTIFIED ETHICAL HACKER

STUDY GUIDE

Includes interactive online learning environment and study tools:

750 practice questions

100 electronic flashcards

Searchable key term glossary

RIC MESSIER, CEH, GSEC, CISSP

SYBEX
A Wiley Brand

CEH™ v12

Certified Ethical Hacker Study Guide

CEH™ v12

Certified Ethical Hacker Study Guide

Ric Messier, CEH, GSEC, CISSP

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-394-18692-1
ISBN: 978-1-394-18687-7 (ebk.)
ISBN: 978-1-394-18691-4 (ebk.)

Library of Congress Control Number: 2023932588

Cover image: © Getty Images Inc./Jeremy Woodhouse
Cover design: Wiley

About the Author

Ric Messier, GCIH, CCSP, GSEC, CEH, CISSP, MS, has entirely too many letters after his name, as though he spends time gathering up strays that follow him home at the end of the day. His interest in information security began in high school but was cemented when he was a freshman at the University of Maine, Orono, when he took advantage of a vulnerability in a jailed environment to break out of the jail and gain elevated privileges on an IBM mainframe in the early 1980s. His first experience with Unix was in the mid-1980s and with Linux in the mid-1990s. Ric is an author, trainer, educator, and security professional with multiple decades of experience. He is currently a Principal Consultant with Mandiant and has developed graduate programs and courses in information security at different colleges and universities.

About the Technical Editor

James Michael Stewart, CISSP, CEH, CHFI, ECSA, CND, ECIH, CySA+, PenTest+, CASP+, Security+, Network+, A+, CISM, and CFR, has been writing and training for more than 25 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on internet security and ethical hacking/penetration testing. He is the author of and contributor to more than 75 books on security certification, Microsoft topics, and network administration, including *CompTIA Security+ Review Guide*. More information about Michael can be found at his website, `www.impactonline.com`.

Contents at a Glance

Introduction		*xvii*
Assessment Test		*xxv*
Chapter 1	Ethical Hacking	1
Chapter 2	Networking Foundations	17
Chapter 3	Security Foundations	59
Chapter 4	Footprinting and Reconnaissance	101
Chapter 5	Scanning Networks	161
Chapter 6	Enumeration	231
Chapter 7	System Hacking	279
Chapter 8	Malware	339
Chapter 9	Sniffing	393
Chapter 10	Social Engineering	435
Chapter 11	Wireless Security	471
Chapter 12	Attack and Defense	511
Chapter 13	Cryptography	549
Chapter 14	Security Architecture and Design	581
Chapter 15	Cloud Computing and the Internet of Things	611
Appendix	Answers to Review Questions	661
Index		*699*

Contents

Introduction *xvii*

Assessment Test *xxv*

Chapter 1 Ethical Hacking 1

Overview of Ethics 2
Overview of Ethical Hacking 5
Attack Modeling 6
- Cyber Kill Chain 7
- Attack Lifecycle 8
- MITRE ATT&CK Framework 10

Methodology of Ethical Hacking 12
- Reconnaissance and Footprinting 12
- Scanning and Enumeration 12
- Gaining Access 13
- Maintaining Access 14
- Covering Tracks 14

Summary 15

Chapter 2 Networking Foundations 17

Communications Models 19
- Open Systems Interconnection 20
- TCP/IP Architecture 23

Topologies 24
- Bus Network 24
- Star Network 25
- Ring Network 26
- Mesh Network 27
- Hybrid 28

Physical Networking 29
- Addressing 29
- Switching 30

IP 31
- Headers 32
- Addressing 34
- Subnets 35

TCP 37
UDP 40
Internet Control Message Protocol 41

Network Architectures 42
Network Types 43
Isolation 44
Remote Access 45
Cloud Computing 46
Storage as a Service 47
Infrastructure as a Service 48
Platform as a Service 49
Software as a Service 51
Internet of Things 53
Summary 54
Review Questions 56

Chapter 3 Security Foundations 59

The Triad 61
Confidentiality 61
Integrity 63
Availability 64
Parkerian Hexad 65
Information Assurance and Risk 66
Policies, Standards, and Procedures 69
Security Policies 69
Security Standards 70
Procedures 71
Guidelines 72
Organizing Your Protections 72
Security Technology 75
Firewalls 76
Intrusion Detection Systems 80
Intrusion Prevention Systems 83
Endpoint Detection and Response 84
Security Information and Event Management 86
Being Prepared 87
Defense in Depth 87
Defense in Breadth 89
Defensible Network Architecture 90
Logging 91
Auditing 93
Summary 95
Review Questions 96

Chapter 4 Footprinting and Reconnaissance 101

Open Source Intelligence 103
Companies 103
People 112

Social Networking 115
Domain Name System 129
Name Lookups 130
Zone Transfers 136
Passive DNS 138
Passive Reconnaissance 142
Website Intelligence 145
Technology Intelligence 150
Google Hacking 150
Internet of Things (IoT) 152
Summary 154
Review Questions 157

Chapter 5 Scanning Networks 161

Ping Sweeps 163
Using *fping* 163
Using MegaPing 165
Port Scanning 167
nmap 168
masscan 184
MegaPing 186
Metasploit 188
Vulnerability Scanning 190
OpenVAS 192
Nessus 203
Looking for Vulnerabilities with Metasploit 209
Packet Crafting and Manipulation 210
hping 211
packETH 214
fragroute 217
Evasion Techniques 218
Evasion with *nmap* 221
Protecting and Detecting 223
Summary 224
Review Questions 226

Chapter 6 Enumeration 231

Service Enumeration 233
Countermeasures 236
Remote Procedure Calls 236
SunRPC 237
Remote Method Invocation 239
Server Message Block 242
Built-in Utilities 243
nmap Scripts 247

NetBIOS Enumerator 249
Metasploit 250
Other Utilities 254
Countermeasures 257
Simple Network Management Protocol 258
Countermeasures 259
Simple Mail Transfer Protocol 260
Countermeasures 263
Web-Based Enumeration 264
Countermeasures 271
Summary 272
Review Questions 274

Chapter 7 System Hacking 279

Searching for Exploits 281
System Compromise 285
Metasploit Modules 286
Exploit-DB 290
Gathering Passwords 292
Password Cracking 295
John the Ripper 296
Rainbow Tables 298
Kerberoasting 300
Client-Side Vulnerabilities 305
Living Off the Land 307
Fuzzing 308
Post Exploitation 313
Evasion 313
Privilege Escalation 314
Pivoting 319
Persistence 322
Covering Tracks 326
Summary 332
Review Questions 334

Chapter 8 Malware 339

Malware Types 341
Virus 341
Worm 342
Trojan 344
Botnet 344
Ransomware 345
Dropper 347

Fileless Malware 348
Polymorphic Malware 348
Malware Analysis 349
Static Analysis 350
Dynamic Analysis 361
Automated Malware Analysis 370
Creating Malware 371
Writing Your Own 372
Using Metasploit 375
Obfuscating 381
Malware Infrastructure 382
Antivirus Solutions 384
Persistence 385
Summary 386
Review Questions 388

Chapter 9 Sniffing 393

Packet Capture 394
tcpdump 395
tshark 401
Wireshark 403
Berkeley Packet Filter 408
Port Mirroring/Spanning 410
Detecting Sniffers 410
Packet Analysis 412
Spoofing Attacks 417
ARP Spoofing 418
DNS Spoofing 422
DHCP Starvation Attack 424
sslstrip 425
Spoofing Detection 426
Summary 428
Review Questions 430

Chapter 10 Social Engineering 435

Social Engineering 436
Pretexting 438
Social Engineering Vectors 440
Identity Theft 441
Physical Social Engineering 442
Badge Access 442
Man Traps 444
Biometrics 445
Phone Calls 446

Baiting 447
Tailgating 448
Phishing Attacks 448
Contact Spamming 452
Quid Pro Quo 452
Social Engineering for Social Networking 453
Website Attacks 454
Cloning 454
Rogue Attacks 457
Wireless Social Engineering 458
Automating Social Engineering 461
Summary 464
Review Questions 466

Chapter 11 Wireless Security 471

Wi-Fi 472
Wi-Fi Network Types 474
Wi-Fi Authentication 477
Wi-Fi Encryption 478
Bring Your Own Device 483
Wi-Fi Attacks 484
Bluetooth 495
Scanning 496
Bluejacking 498
Bluesnarfing 498
Bluebugging 498
Bluedump 499
Bluesmack 499
Mobile Devices 499
Mobile Device Attacks 500
Summary 504
Review Questions 506

Chapter 12 Attack and Defense 511

Web Application Attacks 512
OWASP Top 10 Vulnerabilities 514
Web Application Protections 524
Denial-of-Service Attacks 526
Bandwidth Attacks 527
Slow Attacks 529
Legacy 531
Application Exploitation 531
Buffer Overflow 532
Heap Spraying 534
Application Protections and Evasions 535

Lateral Movement 536
Defense in Depth/Defense in Breadth 538
Defensible Network Architecture 540
Summary 542
Review Questions 544

Chapter 13 Cryptography 549

Basic Encryption 551
Substitution Ciphers 551
Diffie–Hellman 553
Symmetric Key Cryptography 555
Data Encryption Standard 555
Advanced Encryption Standard 556
Asymmetric Key Cryptography 558
Hybrid Cryptosystem 559
Nonrepudiation 559
Elliptic Curve Cryptography 560
Certificate Authorities and Key Management 562
Certificate Authority 562
Trusted Third Party 565
Self-Signed Certificates 566
Cryptographic Hashing 569
PGP and S/MIME 571
Disk and File Encryption 572
Summary 576
Review Questions 578

Chapter 14 Security Architecture and Design 581

Data Classification 582
Security Models 584
State Machine 584
Biba 585
Bell–LaPadula 586
Clark–Wilson Integrity Model 586
Application Architecture 587
n-tier Application Design 588
Service-Oriented Architecture 591
Cloud-Based Applications 593
Database Considerations 595
Security Architecture 598
Zero-Trust Model 602
Summary 604
Review Questions 606

Chapter 15 Cloud Computing and the Internet of Things 611

Cloud Computing Overview 612
Cloud Services 616
Shared Responsibility Model 621
Public vs. Private Cloud 623
Grid Computing 624
Cloud Architectures and Deployment 625
Responsive Design 629
Cloud-Native Design 629
Deployment 631
Dealing with REST 633
Common Cloud Threats 639
Access Management 639
Data Breach 641
Web Application Compromise 642
Credential Compromise 643
Insider Threat 645
Internet of Things 646
Fog Computing 651
Operational Technology 652
The Purdue Model 654
Summary 655
Review Questions 657

Appendix Answers to Review Questions 661

Chapter 2: Networking Foundations 662
Chapter 3: Security Foundations 663
Chapter 4: Footprinting and Reconnaissance 666
Chapter 5: Scanning Networks 669
Chapter 6: Enumeration 672
Chapter 7: System Hacking 675
Chapter 8: Malware 678
Chapter 9: Sniffing 681
Chapter 10: Social Engineering 683
Chapter 11: Wireless Security 686
Chapter 12: Attack and Defense 688
Chapter 13: Cryptography 691
Chapter 14: Security Architecture and Design 693
Chapter 15: Cloud Computing and the Internet of Things 695

Index 699

Introduction

You're thinking about becoming a Certified Ethical Hacker (CEH). No matter what variation of security testing you are performing—ethical hacking, penetration testing, red teaming, or application assessment—the skills and knowledge necessary to achieve this certification are in demand. Even the idea of security testing and ethical hacking is evolving as businesses and organizations begin to have a better understanding of the adversaries they are facing. It's no longer the so-called script kiddies that businesses felt they were fending off for so long. Today's adversary is organized, well-funded, and determined. This means testing requires different tactics.

Depending on who you are listening to, 80–90 percent of attacks today use social engineering. The old technique of looking for technical vulnerabilities in network services is simply not how attackers are getting into networks. Networks that are focused on applying a defense-in-depth approach, hardening the outside, may end up being susceptible to attacks from the inside, which is what happens when desktop systems are compromised. The skills needed to identify vulnerabilities and recommend remediations are evolving, along with the tactics and techniques used by attackers.

This book is written to help you understand the breadth of content you will need to know to obtain the CEH certification. You will find a lot of concepts to provide you with a foundation that can be applied to the skills required for the certification. While you can read this book cover to cover, for a substantial chunk of the subjects, getting hands-on experience is essential. The concepts are often demonstrated through the use of tools. Following along with these demonstrations and using the tools yourself will help you understand the tools and how to use them. Many of the demonstrations are done in Kali Linux, though many of the tools have Windows analogs if you are more comfortable there.

We can't get through this without talking about ethics, though you will find it mentioned in several places throughout the book. This is serious, and not only because it's a huge part of the basis for the certification. It's also essential for protecting yourself and the people you are working for. The short version is do not do anything that would cause damage to systems or your employer. There is much more to it than that, which you'll read more about in Chapter 1, "Ethical Hacking," as a starting point. It's necessary to start wrapping your head around the ethics involved in this exam and profession. You will have to sign an agreement as part of achieving your certification.

At the end of each chapter, you will find a set of questions. This will help you to demonstrate to yourself that you understand the content. Most of the questions are multiple choice, which is the question format used for the CEH exam. These questions, along with the hands-on experience you take advantage of, will be good preparation for taking the exam.

What Is a CEH?

The Certified Ethical Hacker exam is to validate that those holding the certification understand the broad range of subject matter that is required for someone to be an effective

ethical hacker. The reality is that most days, if you are paying attention to the news, you will see a news story about a company that has been compromised and had data stolen, a government that has been attacked, or even enormous denial-of-service attacks, making it difficult for users to gain access to business resources.

The CEH is a certification that recognizes the importance of identifying security issues to get them remediated. This is one way companies can protect themselves against attacks—by getting there before the attackers do. It requires someone who knows how to follow techniques that attackers would normally use. Just running scans using automated tools is insufficient because as good as security scanners may be, they will identify false positives—cases where the scanner indicates an issue that isn't really an issue. Additionally, they will miss a lot of vulnerabilities—false negatives—for a variety of reasons, including the fact that the vulnerability or attack may not be known.

Because companies need to understand where they are vulnerable to attack, they need people who are able to identify those vulnerabilities, which can be very complex. Scanners are a good start, but being able to find holes in complex networks can take the creative intelligence that humans offer. This is why we need ethical hackers. These are people who can take extensive knowledge of a broad range of technical subjects and use it to identify vulnerabilities that can be exploited.

The important part of that two-word phrase, by the way, is "ethical." Companies have protections in place because they have resources they don't want stolen or damaged. When they bring in someone who is looking for vulnerabilities to exploit, they need to be certain that nothing will be stolen or damaged. They also need to be certain that anything that may be seen or reviewed isn't shared with anyone else. This is especially true when it comes to any vulnerabilities that have been identified.

The CEH exam, then, has a dual purpose. It not only tests deeply technical knowledge but also binds anyone who is a certification holder to a code of conduct. Not only will you be expected to know the content and expectations of that code of conduct, you will be expected to live by that code. When companies hire or contract to people who have their CEH certification, they can be assured they have brought on someone with discretion who can keep their secrets and provide them with professional service in order to help improve their security posture and keep their important resources protected.

The Subject Matter

If you were to take the CEH v12 training, you would have to go through the following modules:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDSs, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

As you can see, the range of subjects is broad. Beyond knowing the concepts associated with these topics, you will be expected to know about various tools that may be used to perform the actions associated with the concepts you are learning. You will need to know tools like `nmap` for port scanning, for example. You may need to know proxy-based web application attack tools. For wireless network attacks, you may need to know about the `aircrack-ng` suite of tools. For every module listed, there are potentially dozens of tools that may be used.

The subject matter of the CEH exam is very technical. This is not a field in which you can get by with theoretical knowledge. You will need to have had experience with the methods and tools that are covered within the subject matter for the CEH exam. What you may also have noticed here is that the modules all fall within the different stages mentioned earlier. While you may not necessarily be asked for a specific methodology, you will find that the contents of the exam do generally follow the methodology that the EC-Council believes to be a standard approach.

About the Exam

The CEH exam has much the same parameters as other professional certification exams. You will take a computerized, proctored exam. You will have 4 hours to complete 125 questions. That means you will have, on average, roughly 2 minutes per question. The questions are all multiple choice. The exam can be taken through the ECC Exam Center or at a Pearson VUE center. For details about VUE, please visit `https://home.pearsonvue.com/eccouncil`.

Should you want to take your certification even further, you could go after the CEH Practical exam. For this exam you must perform an actual penetration test and write a report at

the end of it. This demonstrates that in addition to knowing the body of material covered by the exam, you can put that knowledge to use in a practical way. You will be expected to know how to compromise systems and identify vulnerabilities.

To pass the exam, you will have to correctly answer a certain number of questions, though the actual number will vary. The passing grade varies depending on the difficulty of the questions asked. The harder the questions that are asked out of the complete pool of questions, the fewer questions you need to get right to pass the exam. If you get easier questions, you will need to get more of the questions right to pass. There are some sources of information that will tell you that you need to get 70 percent of the questions right, and that may be okay for general guidance and preparation as a rough low-end marker. However, keep in mind that when you sit down to take the actual test at the testing center, the passing grade will vary. The score you will need to achieve will range from 60 to 85 percent.

The good news is that you will know whether you passed before you leave the testing center. You will get your score when you finish the exam, and you will also get a piece of paper indicating the details of your grade. You will get feedback associated with the different scoring areas and how you performed in each of them.

Who Is Eligible

Not everyone is eligible to sit for the CEH exam. Before you go too far down the road, you should check your qualifications. Just as a starting point, you have to be at least 18 years of age. The other eligibility standards are as follows:

- Anyone who has versions 1–7 of the CEH certification. The CEH certification is ANSI certified now, but early versions of the exam were available before the certification. Anyone who wants to take the ANSI-accredited certification who has the early version of the CEH certification can take the exam.
- Minimum of two years of related work experience. Anyone who has the experience will have to pay a nonrefundable application fee of $100.
- Have taken an EC-Council training.

If you meet these qualification standards, you can apply for the certification, along with paying the fee if it is applicable to you (if you take one of the EC-Council trainings, the fee is included). The application will be valid for three months.

Exam Cost

To take the certification exam, you need to pay for a Pearson VUE exam voucher. The cost of this is $1,199. You could also obtain an EC-Council voucher for $950, but that requires that you have taken EC-Council training and can provide a Certificate of Attendance.

EC-Council may change their eligibility, pricing, or exam policies from time to time. We highly encourage you to check for updated policies at the EC-Council website (`https://cert.eccouncil.org/certified-ethical-hacker.html`) when you begin studying for this book and again when you register for this exam.

About EC-Council

The International Council of Electronic Commerce Consultants is more commonly known as the EC-Council (`www.eccouncil.org`). It was created after the airplane attacks that happened against the United States on September 11, 2001. The founder, Jay Bavisi, wondered what would happen if the perpetrators of the attack decided to move from the kinetic world to the digital world. Even beyond that particular set of attackers, the Internet has become a host to a large number of people who are interested in causing damage or stealing information. The economics of the Internet, meaning the low cost of entry into the business, encourage criminals to use it as a means of stealing information, ransoming data, or other malicious acts.

The EC-Council is considered to be one of the largest certifying bodies in the world. It operates in 145 countries and has certified more than 200,000 people. In addition to the CEH, the EC-Council administers a number of other IT-related certifications:

- Certified Network Defender (CND)
- Certified Ethical Hacker Practical
- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Security Analyst Practical
- Licensed Penetration Tester (LPT)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Chief Information Security Officer (CCISO)

One advantage to holding a certification from the EC-Council is that the organization has been accredited by the American National Standards Institute (ANSI). Additionally, and perhaps more importantly for potential certification holders, the certifications from EC-Council are recognized worldwide and have been endorsed by governmental agencies like the National Security Agency (NSA). The Department of Defense Directive 8570 includes the CEH certification. This is important because having the CEH certification means that you could be quickly qualified for a number of positions with the United States government.

The CEH certification provides a bar. This means there is a set of known standards. To obtain the certification, you will need to have met at least the minimal standards. These standards can be relied on consistently. This is why someone with the CEH certification can be trusted. They have demonstrated that they have met known and accepted standards of both knowledge and professional conduct.

Using This Book

This book is structured in a way that foundational material is up front. With this approach, you can make your way in an orderly fashion through the book, one chapter at a time. Technical books can be dry and difficult to get through sometimes, but it's always my goal to try to make them easy to read and I hope entertaining along the way. If you already have a lot of experience, you don't need to take the direct route from beginning to end. You can skip around as you need. No chapter relies on any other. They all stand alone with respect to the content. However, if you don't have the foundation and try to jump to a later chapter, you may find yourself getting lost or confused by the material. All you need to do is jump back to some of the foundational chapters.

Beyond the foundational materials, the book generally follows a fairly standard methodology when it comes to performing security testing. This methodology will be further explained in Chapter 1. As a result, you can follow along with the steps of a penetration test/ethical hacking engagement. Understanding the outline and reason for the methodology will also be helpful to you. Again, though, if you know the material, you can move around as you need.

Additional Study Tools

This book is accompanied by an online learning environment that provides several additional elements. The following items are available among these companion files:

Practice tests All of the questions in this book appear in our proprietary digital test engine—including the 30-question assessment test at the end of this introduction and the 100+ questions that make up the review question sections at the end of each chapter. In addition, there are four bonus exams, each 125 questions.

Electronic "flashcards" The digital companion files include more than 100 questions in flashcard format (a question followed by a single correct answer). You can use these to review your knowledge of the exam objectives.

Glossary The key terms from this book, and their definitions, are available as a fully searchable PDF.

Interactive Online Learning Environment and Test Bank

To start using additional online materials that accompany this book to study for the Certified Ethical Hacker exam, go to `www.wiley.com/go/sybextestprep` and click the link "Click here to register a product" to receive your unique PIN. Once you have the PIN, return to `www.wiley.com/go/sybextestprep`, find your book and click Register or Login, and follow the link to create a new account or add this book to an existing account.

Like all exams, the CEH certification from EC-Council is updated periodically and may eventually be retired or replaced. At some point after EC-Council is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

Objective Map

Table 1.1 contains an objective map to show you at a glance where in the book you can find each objective covered. While there are chapters listed for all of these, there are some objectives that are scattered throughout the book. Specifically, tools, systems, and programs get at least touched on in most of the chapters.

TABLE 1.1 Objective Map

Objective	Chapter
Tasks	
1.1 Systems development and management	7, 14
1.2 Systems analysis and audits	4, 5, 6, 7
1.3 Security testing and vulnerabilities	7, 8
1.4 Reporting	1, 7
1.5 Mitigation	7, 8
1.6 Ethics	1

TABLE 1.1 Objective Map *(continued)*

Objective	Chapter
Knowledge	
2.1 Background	2, 3
2.2 Analysis/assessment	2, 11
2.3 Security	3, 13, 14
2.4 Tools, systems, programs	4, 5, 6, 7
2.5 Procedures/methodology	1, 4, 5, 6, 7, 14
2.6 Regulation/policy	1, 14
2.7 Ethics	1

Let's Get Started!

This book is structured in a way that you will be led through foundational concepts and then through a general methodology for ethical hacking. You can feel free to select your own pathway through the book. Remember, wherever possible, get your hands dirty. Get some experience with tools, tactics, and procedures that you are less familiar with. It will help you a lot.

Take the self-assessment. It may help you get a better idea of how you can make the best use of this book.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Assessment Test

1. Which header field is used to reassemble fragmented IP packets?
   - **A.** Destination address
   - **B.** IP identification
   - **C.** Don't fragment bit
   - **D.** ToS field

2. If you were to see the following in a packet capture, what would you expect was happening?

   ```
   ' or 1=1;
   ```

   - **A.** Cross-site scripting
   - **B.** Command injection
   - **C.** SQL injection
   - **D.** XML external entity injection

3. What method might you use to successfully get malware onto a mobile device?
   - **A.** Through the Apple Store or Google Play Store
   - **B.** External storage on an Android
   - **C.** Third-party app store
   - **D.** Jailbreaking

4. What protocol is used to take a destination IP address and get a packet to a destination on the local network?
   - **A.** DHCP
   - **B.** ARP
   - **C.** DNS
   - **D.** RARP

5. What would be the result of sending the string AAAAAAAAAAAAAAAA into a variable that has been allocated space for 8 bytes?
   - **A.** Heap spraying
   - **B.** SQL injection
   - **C.** Buffer overflow
   - **D.** Slowloris attack

6. If you were to see the subnet mask 255.255.248.0, what CIDR notation (prefix) would you use to indicate the same thing?
   - **A.** /23
   - **B.** /22
   - **C.** /21
   - **D.** /20

7. What is the primary difference between a worm and a virus?
   - **A.** A worm uses polymorphic code.
   - **B.** A virus uses polymorphic code.
   - **C.** A worm can self-propagate.
   - **D.** A virus can self-propagate.

8. How would you calculate risk?
   - **A.** Probability * loss
   - **B.** Probability * mitigation factor
   - **C.** (Loss + mitigation factor) * (loss/probability)
   - **D.** Loss * mitigation factor

9. How does an evil twin attack work?
   - **A.** Phishing users for credentials
   - **B.** Spoofing an SSID
   - **C.** Changing an SSID
   - **D.** Injecting four-way handshakes

10. To remove malware in the network before it gets to the endpoint, you would use which of the following?
    - **A.** Antivirus
    - **B.** Application layer gateway
    - **C.** Unified threat management appliance
    - **D.** Stateful firewall

11. What is the purpose of a security policy?
    - **A.** Providing high-level guidance on the role of security
    - **B.** Providing specific direction to security workers
    - **C.** Increasing the bottom line of a company
    - **D.** Aligning standards and practices

12. What has been done to the following string?

    ```
    %3Cscript%3Ealert('wubble');%3C/script%3E
    ```

    - **A.** Base64 encoding
    - **B.** URL encoding
    - **C.** Encryption
    - **D.** Cryptographic hashing

13. What would you get from running the command `dig ns domain.com`?

A. Mail exchanger records for `domain.com`

B. Name server records for `domain.com`

C. Caching name server for `domain.com`

D. IP address for the hostname `ns`

14. What technique would you ideally use to get all of the hostnames associated with a domain?

A. DNS query

B. Zone copy

C. Zone transfer

D. Recursive request

15. If you were to notice operating system commands inside a DNS request while looking at a packet capture, what might you be looking at?

A. Tunneling attack

B. DNS amplification

C. DNS recursion

D. XML entity injection

16. What would be the purpose of running a ping sweep?

A. You want to identify responsive hosts without a port scan.

B. You want to use something that is light on network traffic.

C. You want to use a protocol that may be allowed through the firewall.

D. All of the above.

17. How many functions are specified by NIST's cybersecurity framework?

A. 0

B. 3

C. 5

D. 4

18. What would be one reason not to write malware in Python?

A. The Python interpreter is slow.

B. The Python interpreter may not be available.

C. There is inadequate library support.

D. Python is a hard language to learn.

19. If you saw the following command line, what would you be capturing?

```
tcpdump -i eth2 host 192.168.10.5
```

A. Traffic just from 192.168.10.5

B. Traffic to and from 192.168.10.5

C. Traffic just to 192.168.10.5

D. All traffic other than from 192.168.10.5

20. What is Diffie-Hellman used for?

A. Key management

B. Key isolation

C. Key exchange

D. Key revocation

21. Which social engineering principle may allow a phony call from the help desk to be effective?

A. Social proof

B. Imitation

C. Scarcity

D. Authority

22. How do you authenticate with SNMPv1?

A. Username/password

B. Hash

C. Public string

D. Community string

23. What is the process Java programs identify themselves to if they are sharing procedures over the network?

A. RMI registry

B. RMI mapper

C. RMI database

D. RMI process

24. What do we call an ARP response without a corresponding ARP request?

A. Is-at response

B. Who-has ARP

C. Gratuitous ARP

D. IP response