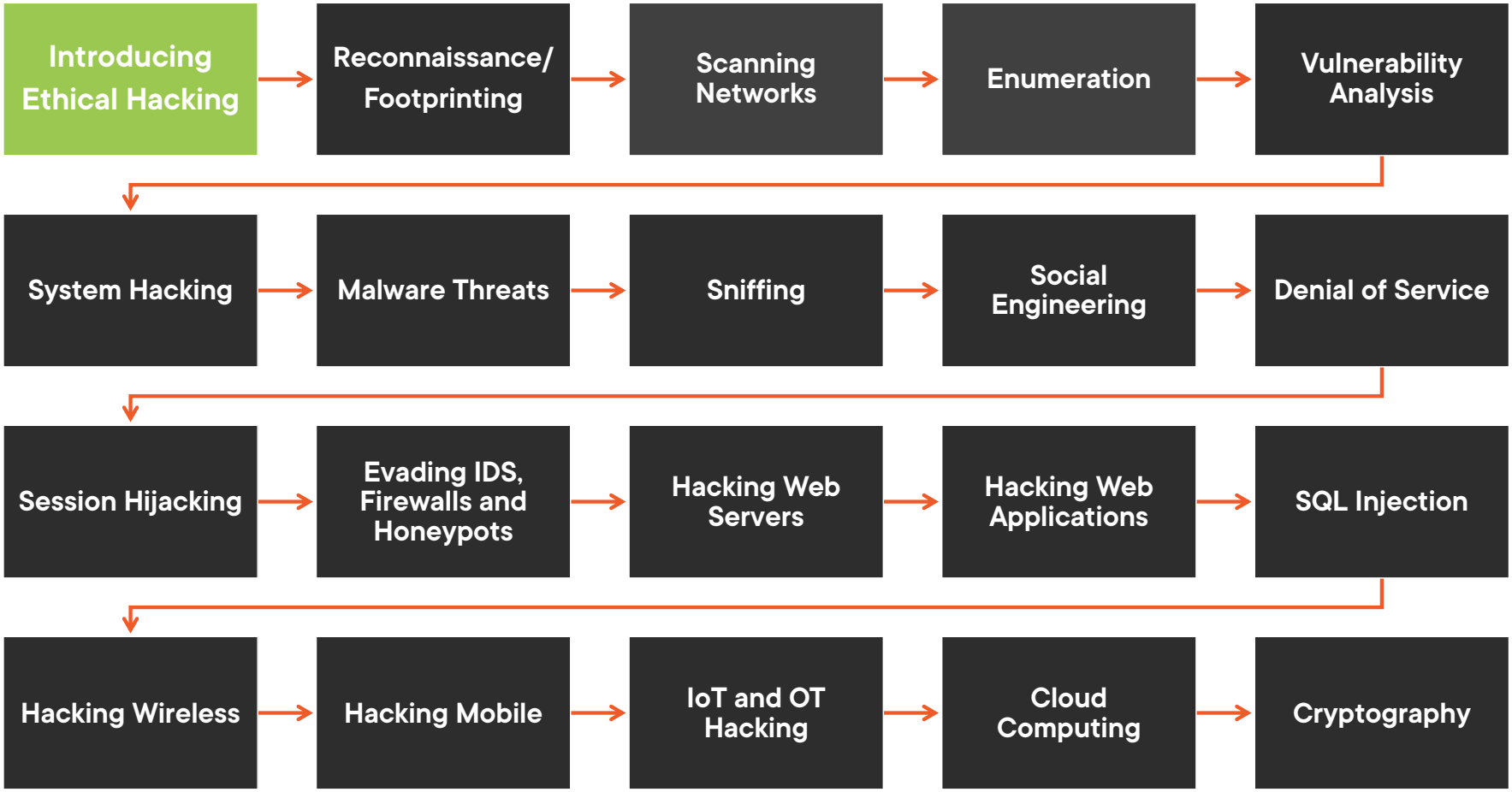
Ethical Hacking: Introducing Ethical Hacking

Classifying Information Security

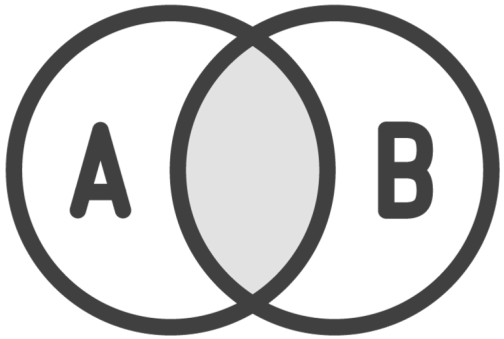
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

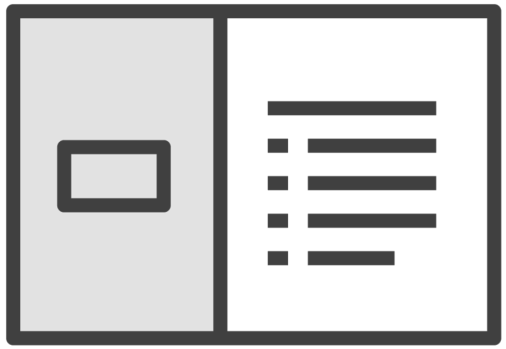
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Ethical Hacking Series

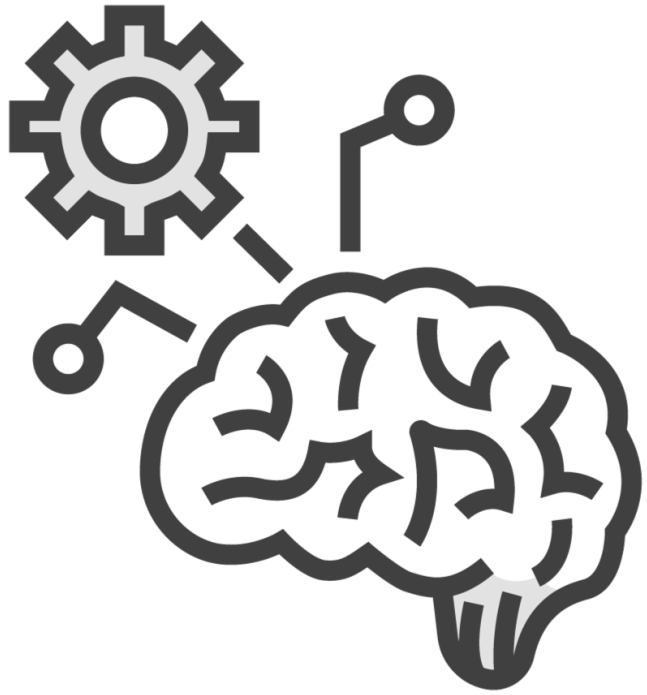


The Method behind My Madness





The Method Behind My Madness



CEH Exam Study Tips

Survey Results

Higher Salaries

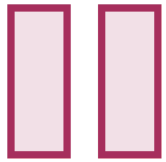
70% held two certifications

Gives you an edge

Dale's Study Tips

Study space

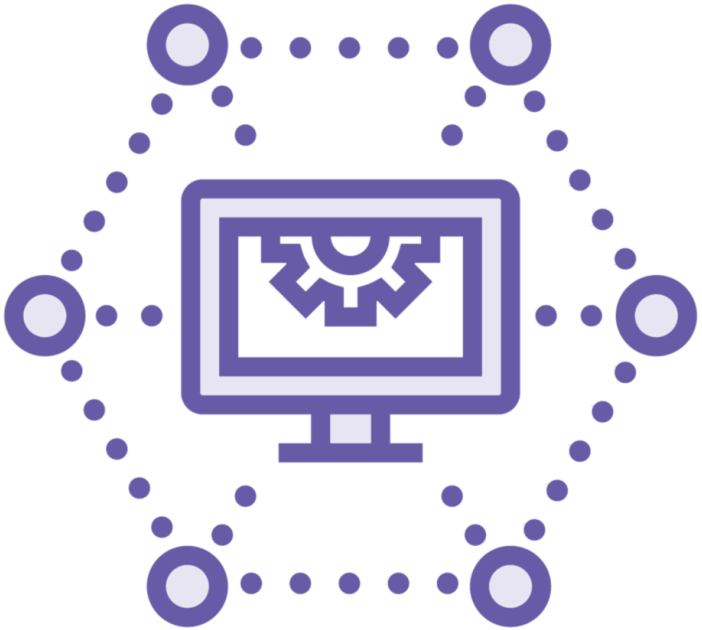
Take notes



Pause, think, repeat

Be kind and rewind

Dale's Study Tips



Life moves pretty fast. If you don't stop and look around once in a while, you could miss it.

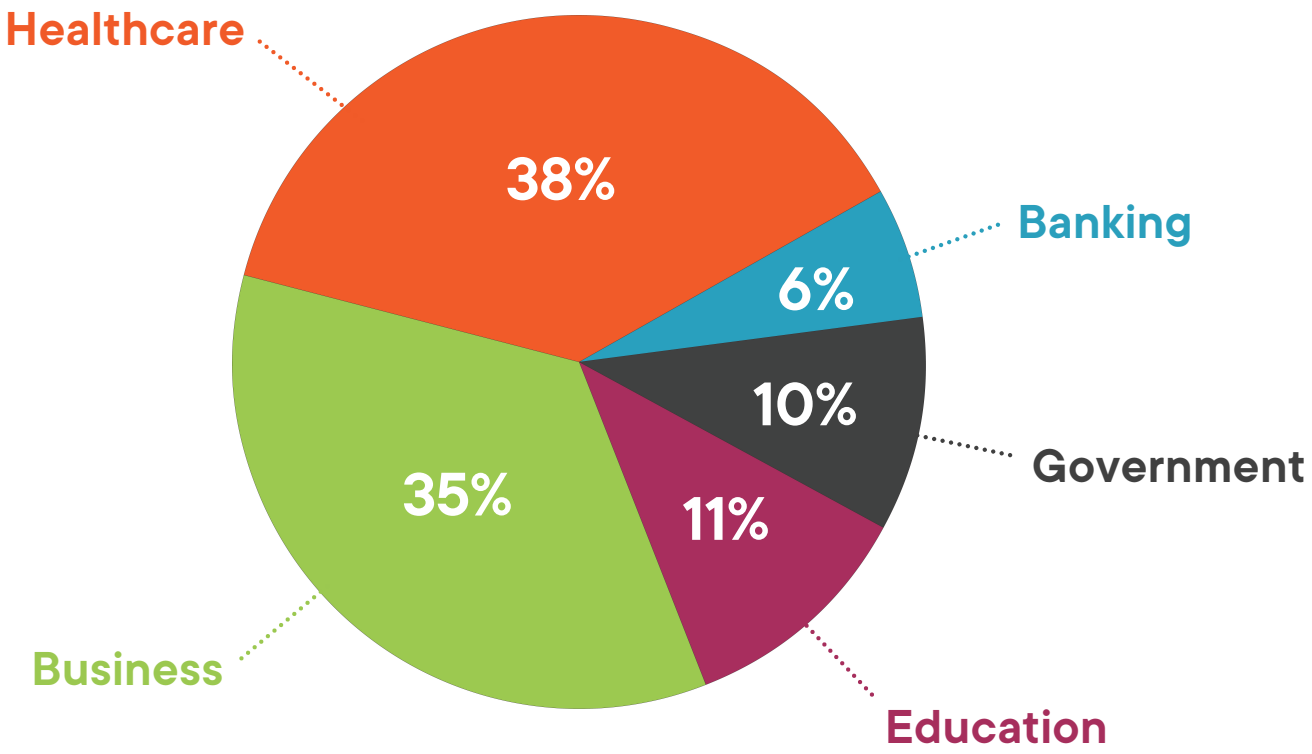
-Ferris Bueller

Ethical Hacking?

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu, The Art of War

Breaches by Industry



Some Interesting Stats

There is a hacker attack every 39 seconds

300,000 new malware is created every day.

The cybersecurity budget in the US is $14.98 billion

Cybercrime is more profitable than the global illegal drug trade

Russian hackers can infiltrate a computer network in 18 minutes

Some Interesting Stats

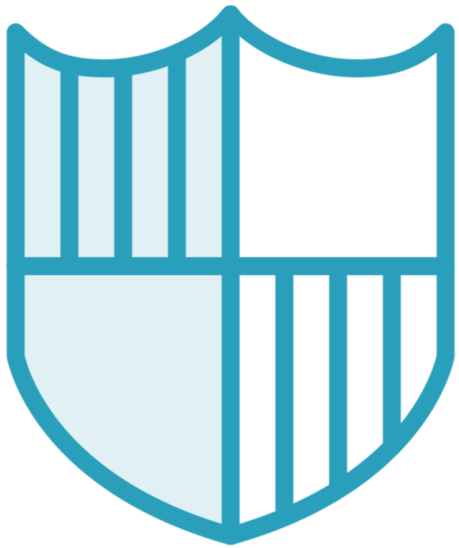
65% of companies have over 1,000 stale user accounts

92% of ATMs are vulnerable to hacker attacks

Ransomware attacks happen every 14 seconds

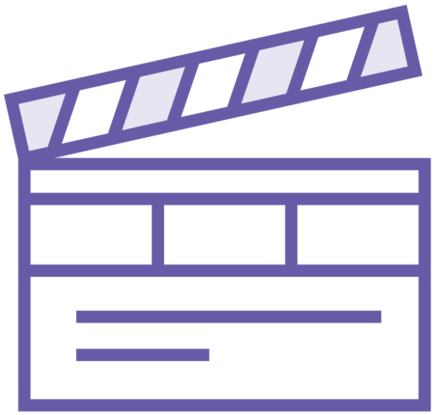
65% of large companies have more than 500 employees who have never changed their passwords

More than 77% of organizations do not have a cyber security incident response plan



How protected do you feel?

A Little About the CEH Program



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

Tom Hanks -League of Their Own, 1992

What Certification Brings You

Internationally recognized

Industry standard

Meets DOD Directive 8570.1

Benefits your resume

High demand certification

Who Should Watch This Series?

- **Security officers**
- **Auditors**
- **Security professionals**
- **Site administrators**
- **Anyone that might be worried about being hacked**

What's Expected of You

Code of Ethics

https://www.eccouncil.org/support/code-of-ethics

What's Expected of You

- **Privacy**
- **Intellectual property**
- **Disclosure**
- **Areas of expertise**
- **Unauthorized usage**
- **Illegal activities**
- **Authorization**
- **No Villains allowed**

Source: https://www.eccouncil.org/code-of-ethics

Just because you can, doesn't mean you can.

-Dale Meredith

Understanding Information Security

Fundamentals of Information Security

Authenticity

Integrity

Availability

Confidentiality

Non-repudiation

Types of Attacks

Attacks = Motive + Method + Vulnerability

Disrupt business continuity

Steal info/data

Create fear and chaos

Financial losses

Publicize political or religious beliefs

Attacks = Motive + Method + Vulnerability

Achieve a state's military objectives

Reputation of target

Revenge

Ransom

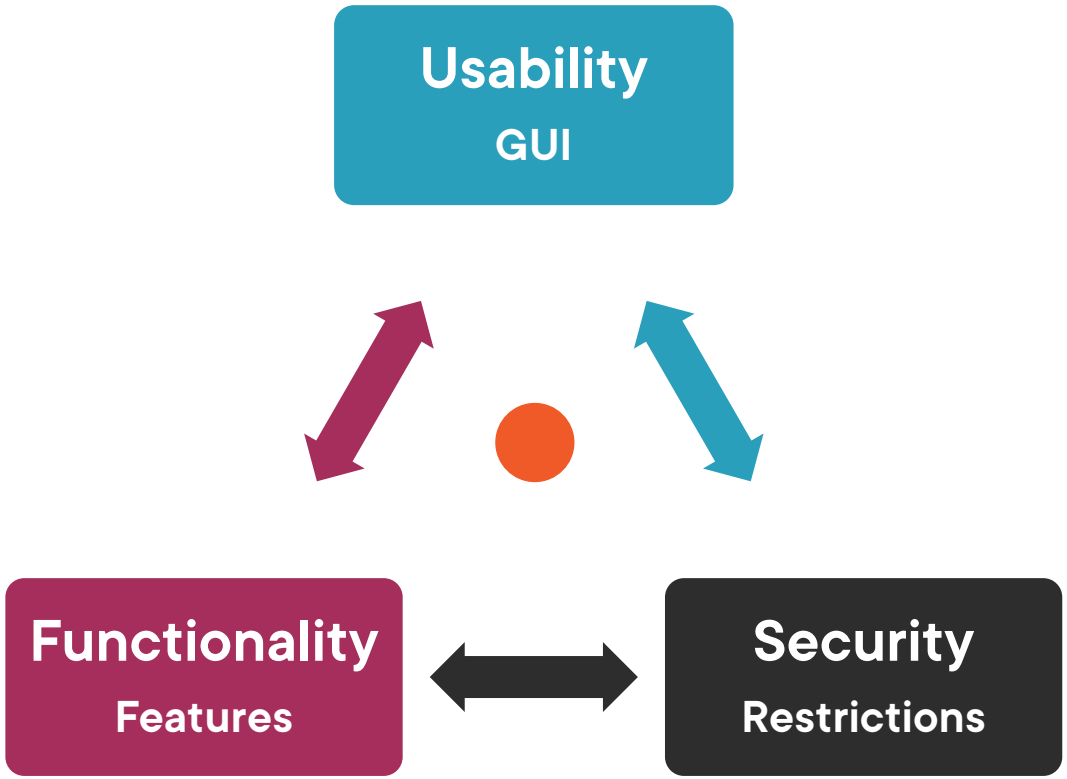
Classifications

- **Passive attacks**
- **Active attacks**
- **Close-in attacks**
- **Insider attacks**
- **Distribution attacks**

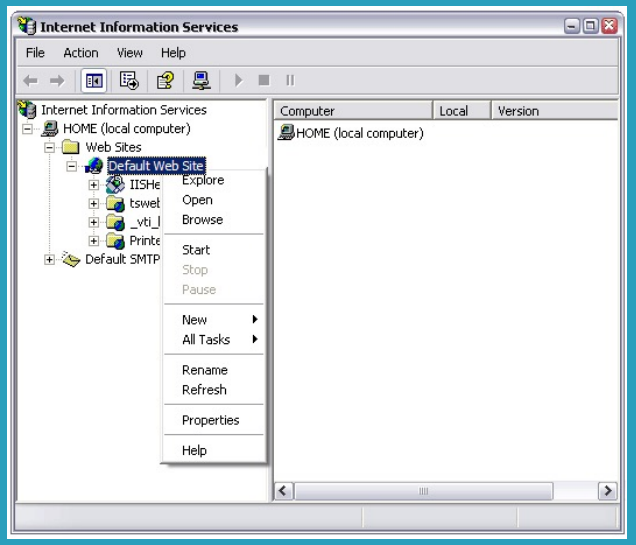
The Solarwinds Attack

The Technology Triangle

The Technology Triangle

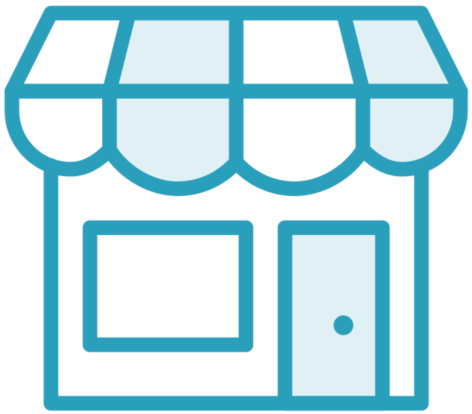


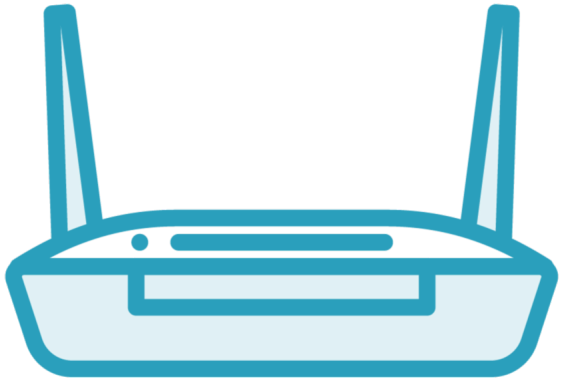
Windows Server 2000 and IIS 5.0



181% increase in vulnerabilities

Usability = Security Risks





Learning Check

Learning Check

- Passive attacks
- Insider attack
- Close-in attack
- Active attack
- Distribution attack

Up Next: Understanding the Attackers and Their Methods