

Comparing Hacking and Ethical Hacking



Dale Meredith

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

dalemeredith.com | Twitter: @dalemeredith | LinkedIn: dalemeredith |

Hacking Concepts

“Hacking is exploiting security controls either in a technical, physical or a human-based element”

Kevin Mitnick

A photograph of two men standing in front of a white wall with red and black text. Both men are wearing glasses and smiling. The man on the left has his arm around the man on the right. They are both wearing lanyards with the word "VERACODE" printed on them.

ANALYZED PRIORITIZED PLANNING

Change the problem

engineering

XBOX

LAN

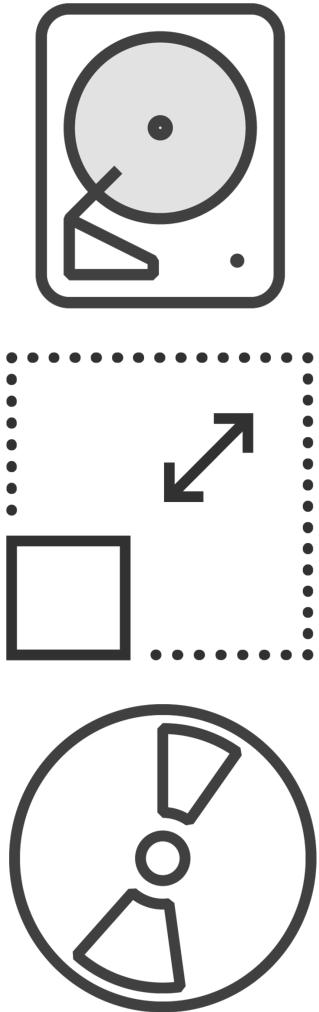
H.D.



O-O

1 } Bank
2 } Select
3 }
4 } Flash Protect





Hacking isn't always nefarious

Types of Hackers

Black Hats

White Hats

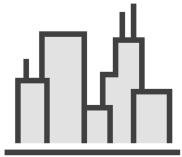
Gray Hats

Suicide Hackers

Script Kiddies



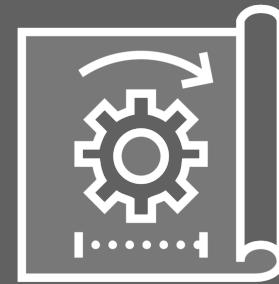
Spy, Cyber and State-Sponsored



Organized crime and big corporations



Driven by political or religious agendas





Spy or Terrorist



State-Sponsored

Who's a Hacker?



Excellent
computer skills



Hobbyist



Curious

Hacktivism



Drive

Political, social,
ideology, vandalism,
protest, humiliate



Political Agenda

Defacing or
disabling websites



Targets

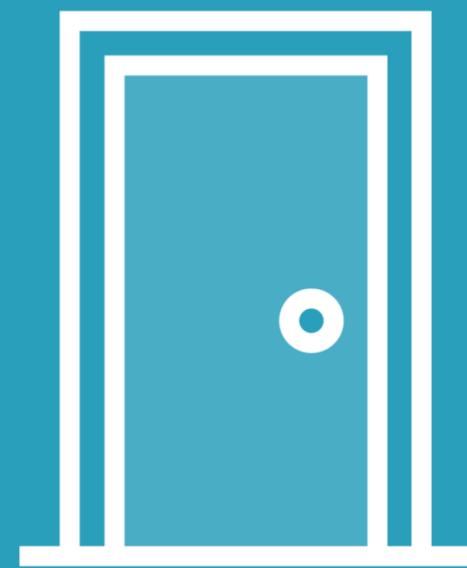
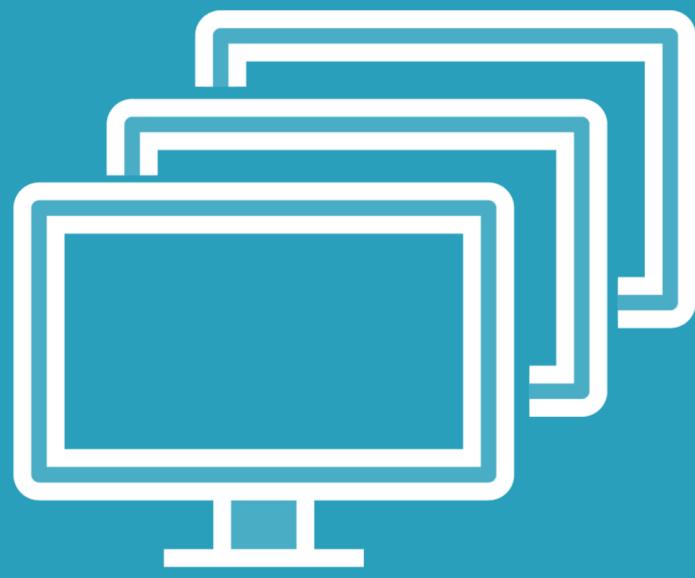
Government agencies,
multinational corps,
“wrong”

Hacking

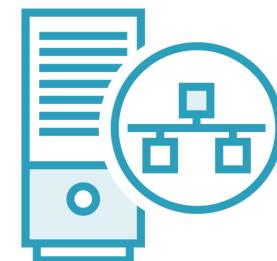
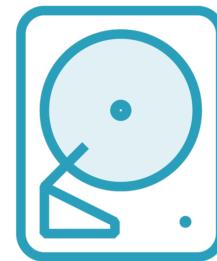
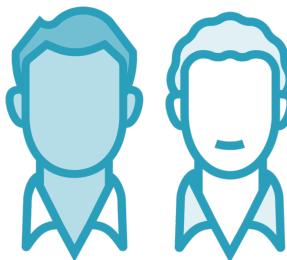
Exploiting a systems vulnerabilities and security controls to gain access to system resources and features, outside the creator's original purpose.

Hacking Phases

What's the most secure system?



Story Time with Dale



Anticipate all forms of attack

Your Job



Discourage



Detour



Misdirect



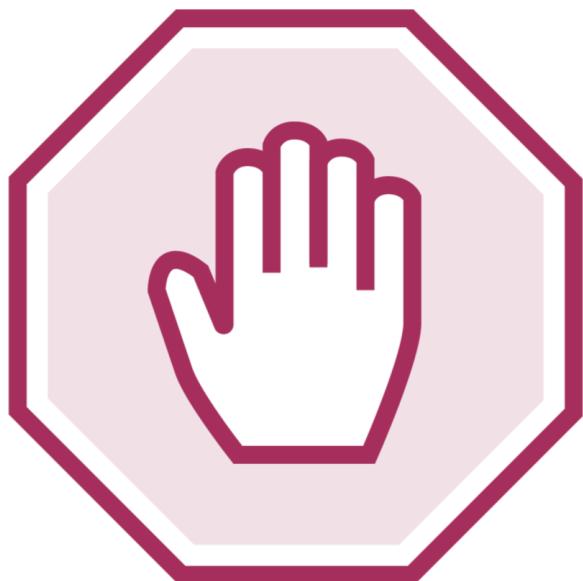
Slowdown

What's the most secure system?

The one that's never built!

Everything is hackable

You Can't Stop “Them”



Your job is to discourage, misdirect and slow them down

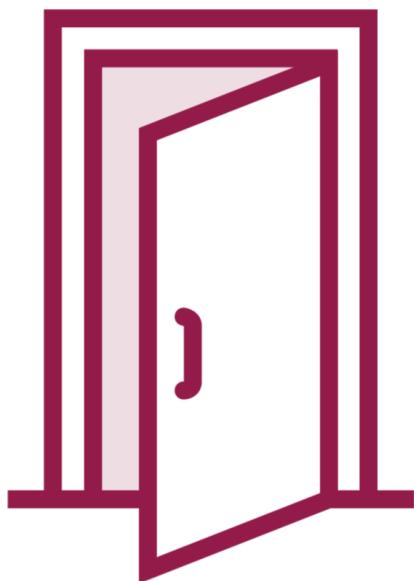
You Can't Stop “Them”



Your job is to discourage, misdirect and slow them down

Time is NOT on your side

You Can't Stop “Them”

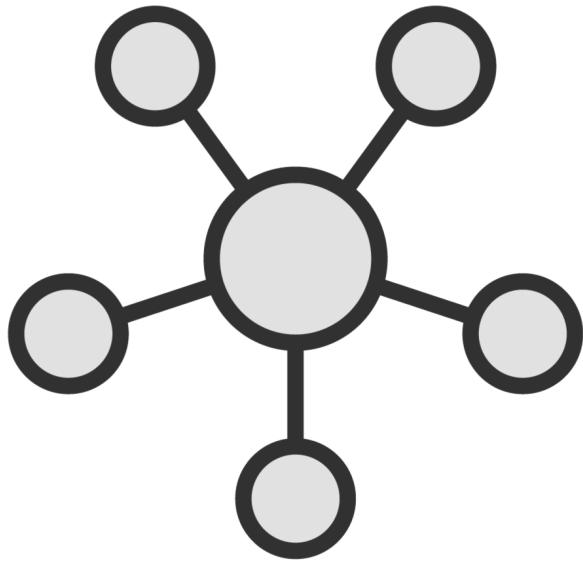


Your job is to discourage, misdirect and slow them down

Time is NOT on your side

Attackers only have to find one opening

You Can't Stop “Them”

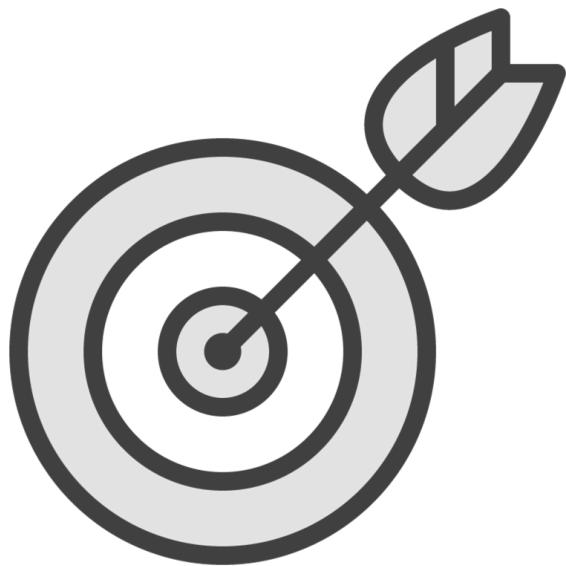


Your job is to discourage, misdirect and slow them down

Time is NOT on your side

Attackers only have to find one opening

You must cover all of them



The Phases

Reconnaissance

Scanning

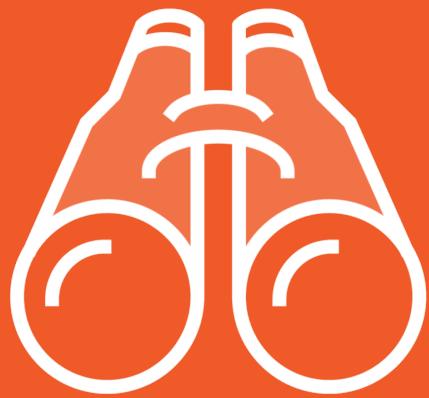
Gaining access

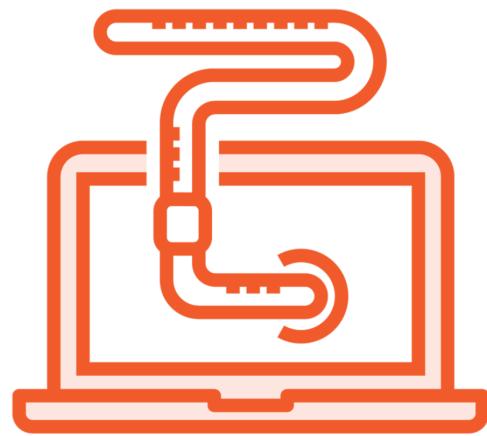
Maintaining access

Clearing tracks

Phase 1: Reconnaissance

Reconnaissance

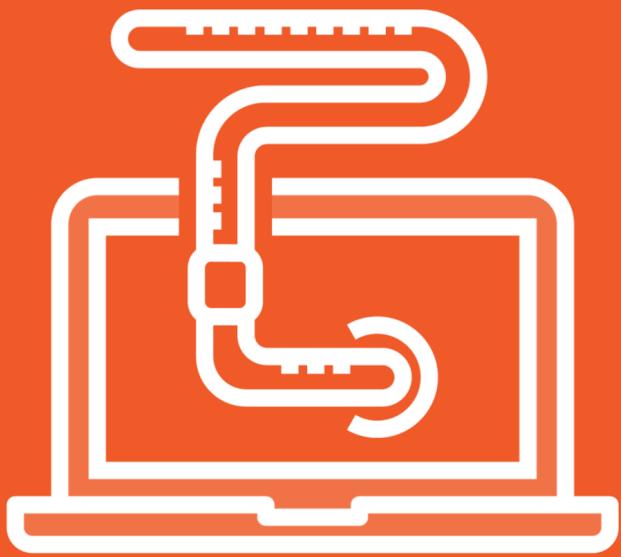




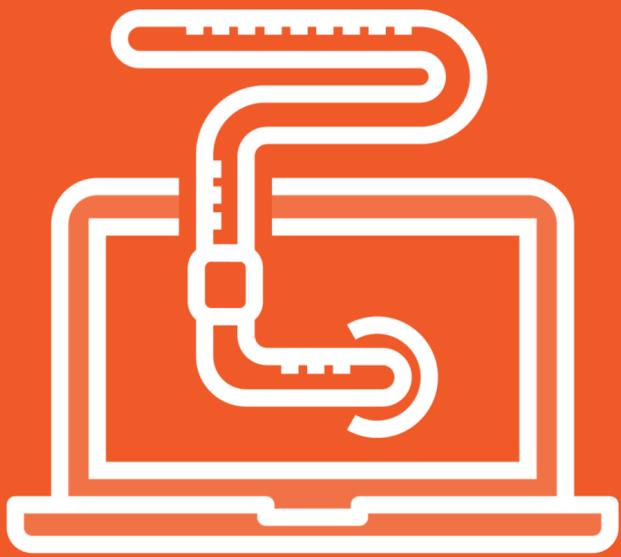
Passive



Active



No direct interaction with the target



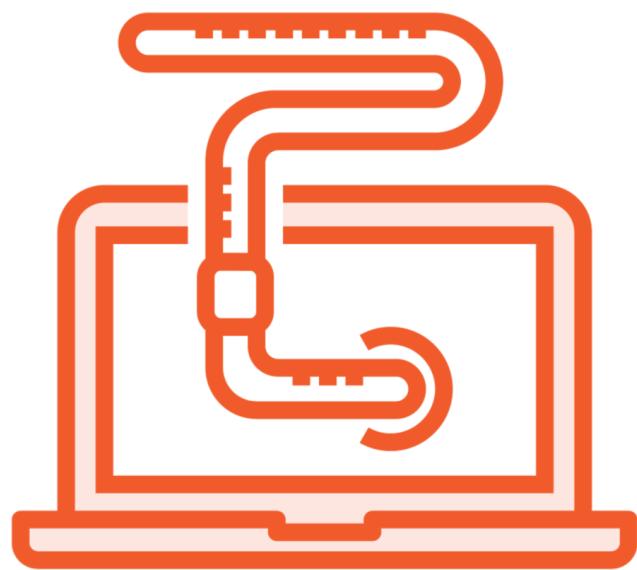
No direct interaction with the target
Research the company



Direct interaction with the target



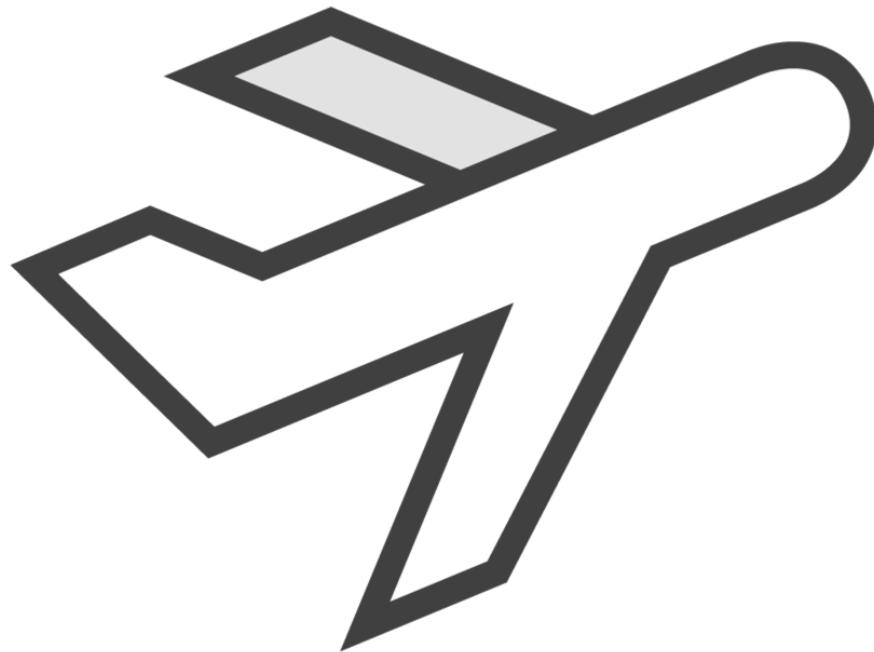
Direct interaction with the target
Engage and scans the network



Social Engineering

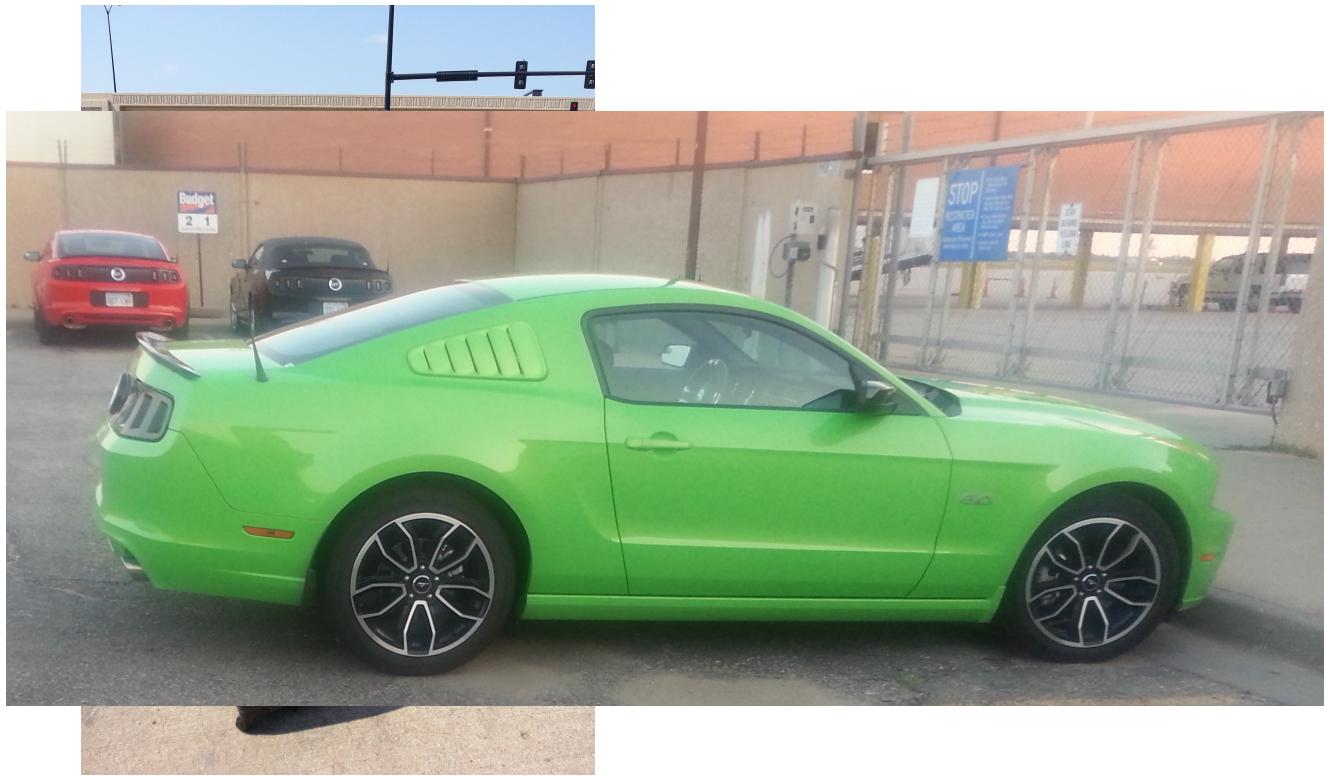
Story Time with Dale

Story Time with Dale



Story Time with Dale



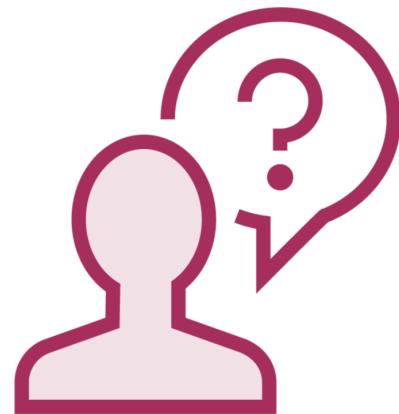




Marketers and advertisers are masters at social engineering









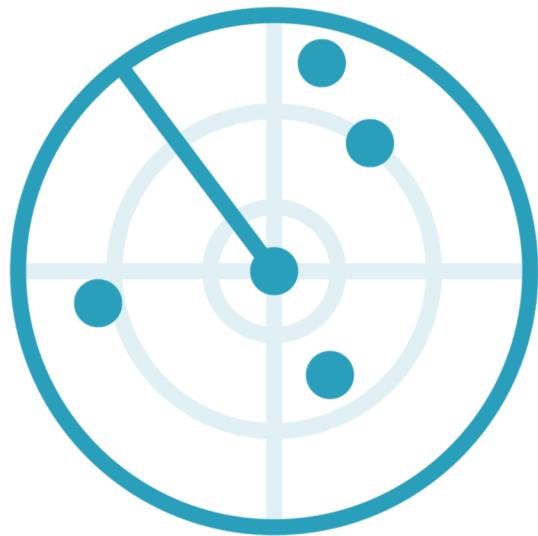






Phase 2: Scanning

Phase 2: Scanning



Gather info

- ID systems
- Vulnerabilities

Tools Used

- Port scanners
- Vulnerability scanners

Phase 3: Gaining Access

Phase 3: Gaining Access

Via network

Via OS

Via application

What is the goal?

Goals



Access data



Reconfigure or crash a system



Exhaust the resources

Password cracking

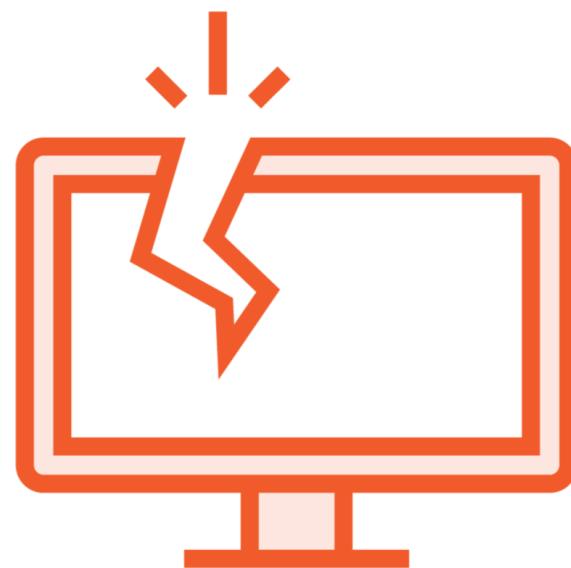
Buffer overflows

in

Session hijacking

Denial of service

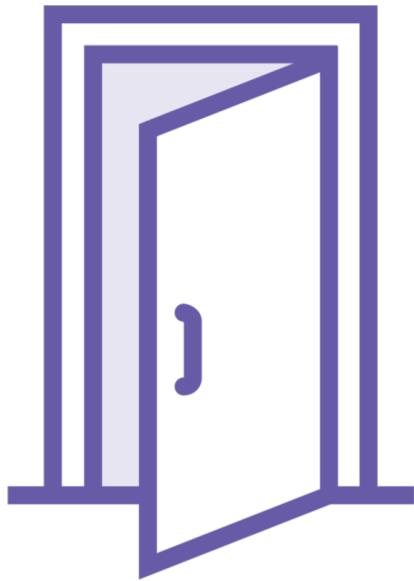




Escalate Privileges

Phase 4: Maintaining Access

Phase 4: Maintaining Access



PWNing the system

Use system as a launch pad

Inject backdoor/trojans

- Used to revisit
- Used to sniff/monitor network

Use resources

Harden up

Phase 5: Clearing Tracks

Phase 5: Clearing Tracks

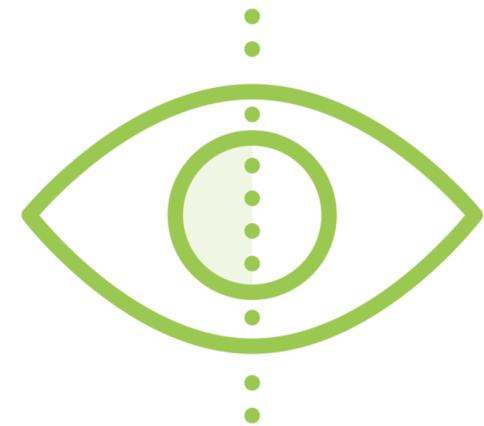
“These are not the drones that you were looking for...”



Destroy proof



Hide my stuff



Cyber blind

So What's Ethical Hacking?

Involves the use of hacking methods and tools to discover weaknesses for system security

What Skills Should an Ethical Hacker Have?



- Expert with programs and networks**
- Proficient with vulnerability research**
- Mastery with diverse hacking techniques**
- Follow a strict code of conduct**
- Explicit permissions in writing**
- Use the same tactics and strategies**
- Just because you can, doesn't mean you can**
- Report all of your results**

Let's Talk About the Labs

Let's Talk About the Labs

The screenshot shows a course library for "Ethical Hacking Fundamentals" by Dale Meredith. The course has been watched for 25h 35m of 81h 29m, which is 31% complete. Below the main course, there are several sub-courses listed:

- Ethical Hacking: Understanding Ethical Hacking
- Ethical Hacking: Reconnaissance/Footprinting
- Ethical Hacking: Scanning Networks
- Ethical Hacking: Enumeration
- Discover and Enumerate Targets with Nmap
- Ethical Hacking: Vulnerability Analysis
- Ethical Hacking: System Hacking
- Ethical Hacking: Malware

The screenshot shows a course details page for "Building a Cybersecurity Home Lab Environment" by Dale Meredith. The course summary states: "This course will teach you how to set up a hacking lab environment for all your security research, hacking tools, and training you've always wanted to do." The course is currently at 0% completion.

Course author: Dale Meredith (Certified Ethical Hacker/Instructor EC-Council for the past 15 years, and Microsoft Certified Trainer for over 20 years. Dale also has an additional 7 years of senior IT...)

Course info:

- Level: Intermediate
- Rating: ★★★★☆ (18)
- My rating: ★★★★☆
- Duration: 2h 2m
- Released: 6 Aug 2020

Table of contents:

- Course Overview (2m 22s)
- Setting up a Lab Environment (34m 58s)
 - Understanding What You're Trying to Do
 - The Requirements
 - Setting up the Host Machine Using Hyper-V (8m 50s)

Pluralsight Online Labs

Build Your Own Virtual Hacking Lab

Learning Check

Learning Check



Suicide hacker



Gray hat



Script kiddies



Black hat



Hacktivist



Learning Check



Passive reconnaissance



Active reconnaissance



Clearing tracks



Maintaining access



Gaining access



Up Next:
Describing Information Security Controls
