Comparing Hacking and Ethical Hacking

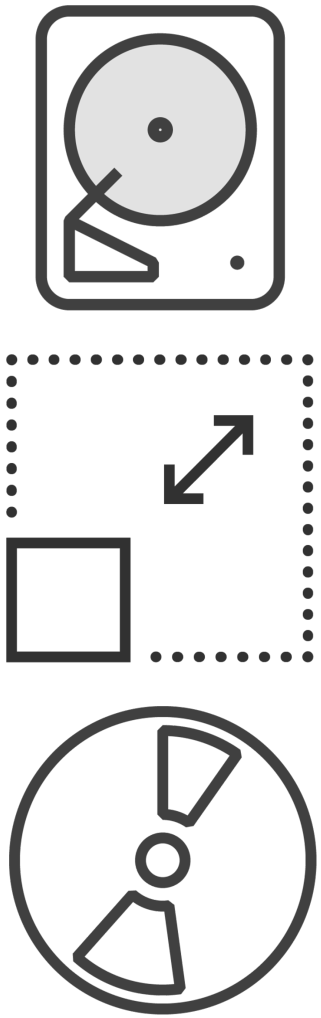
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

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



Hacking isn’t always nefarious

Types of Hackers

Black Hats

White Hats

Gray Hats

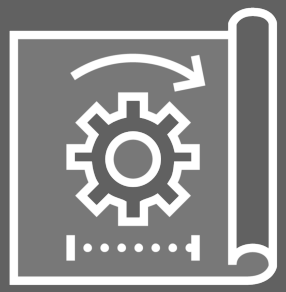
Suicide Hackers

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”

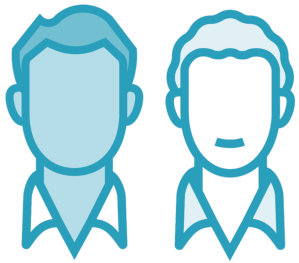
Hacking

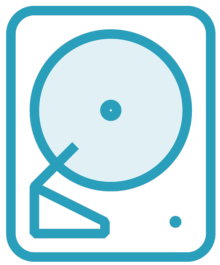
Exploiting a systems vulnerabilities and security controls to gain access to system resources and features, outside the creator's original purpose.

Hacking Phases

What's the most secure system?

Story Time with Dale





Anticipate all forms of attack

Your Job

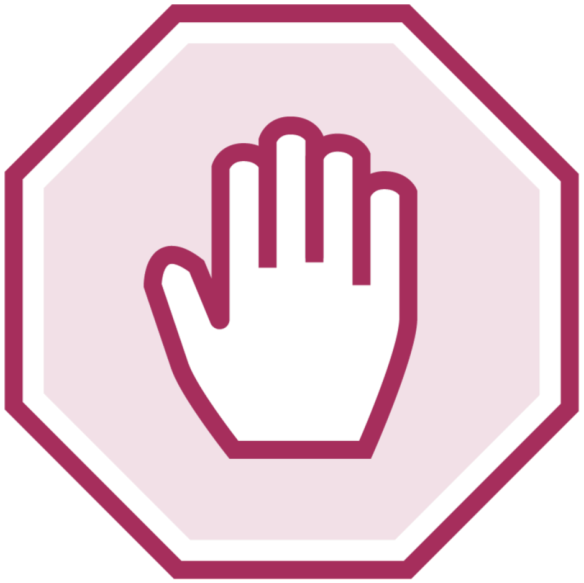
- **Discourage**
- **Detour**
- **Misdirect**
- **Slowdown**

What's the most secure system?

The one that's never built!

Everything is hackable

You Can't Stop "Them"



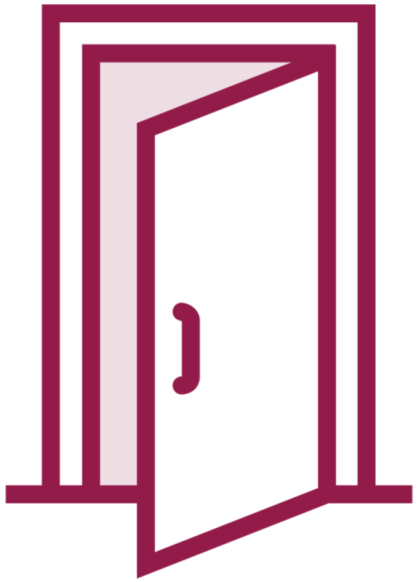
Your job is to discourage, misdirect and slow them down

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"

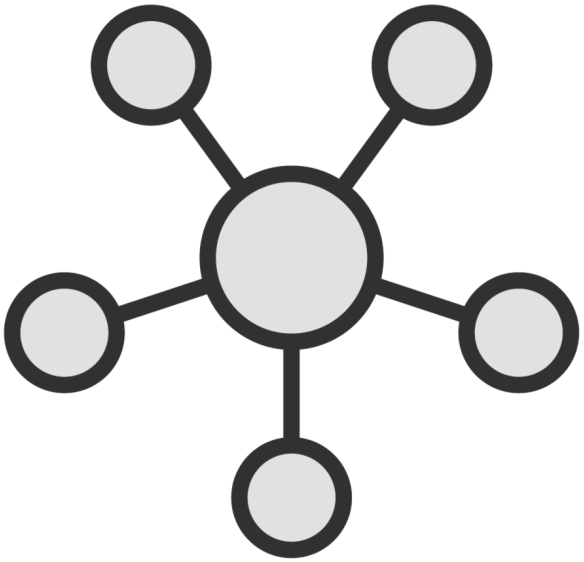


Your job is to discourage, misdirect and slow them down

Time is NOT on your side

Attackers only have to find one opening

You Can't Stop "Them"



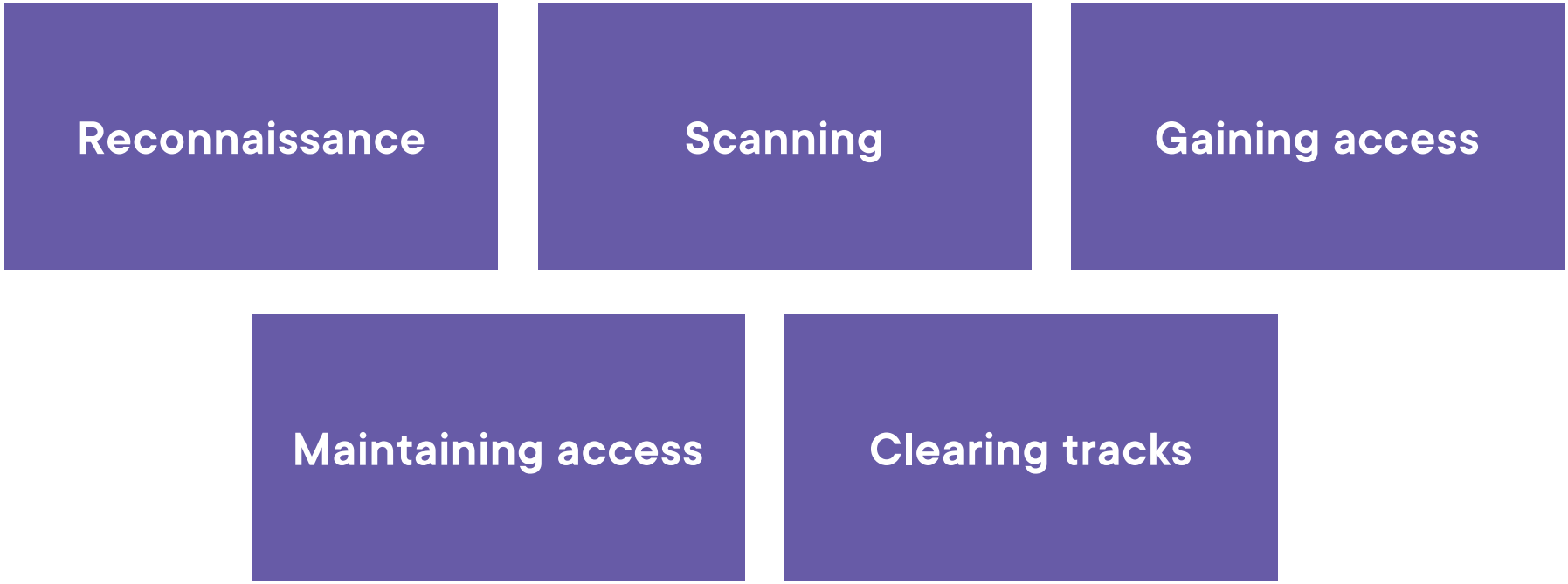
Your job is to discourage, misdirect and slow them down

Time is NOT on your side

Attackers only have to find one opening

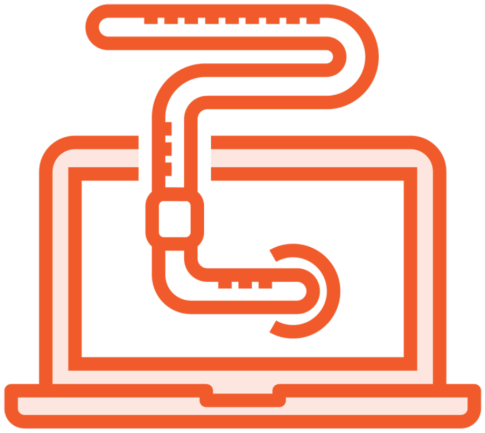
You must cover all of them

The Phases



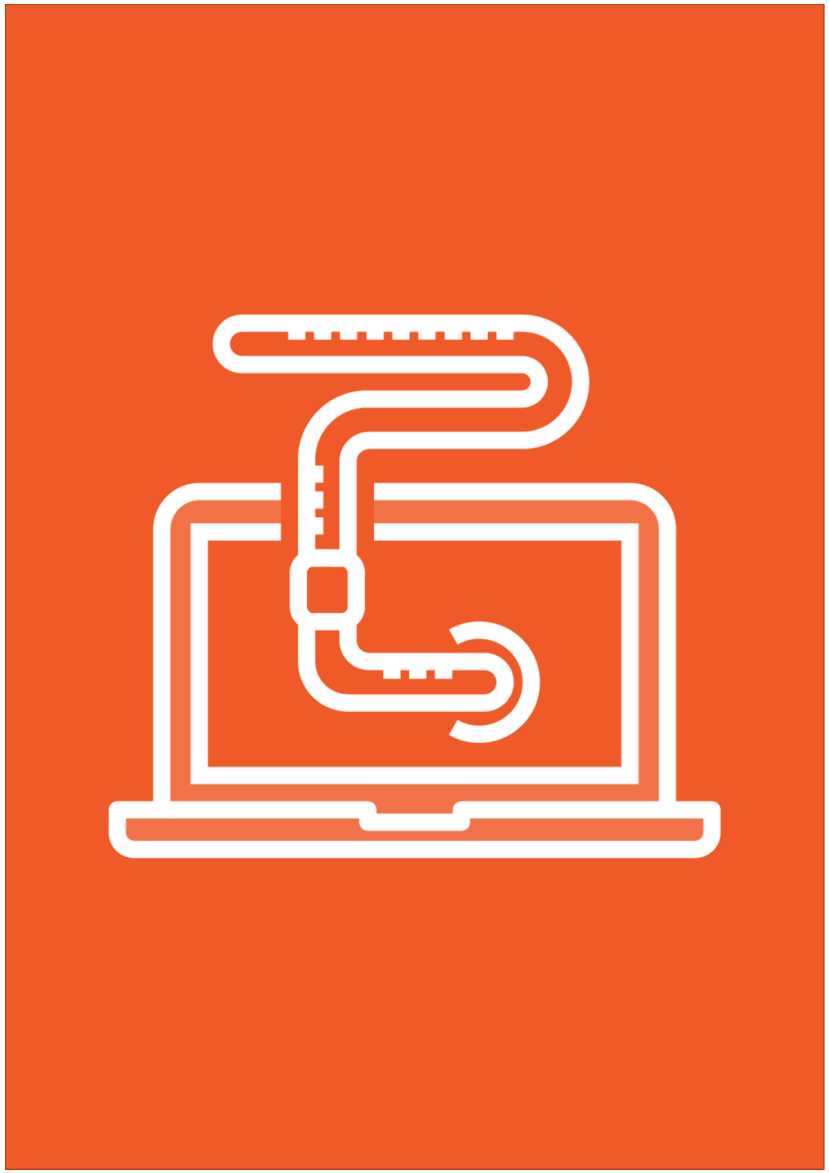
Phase 1: Reconnaissance

Reconnaissance

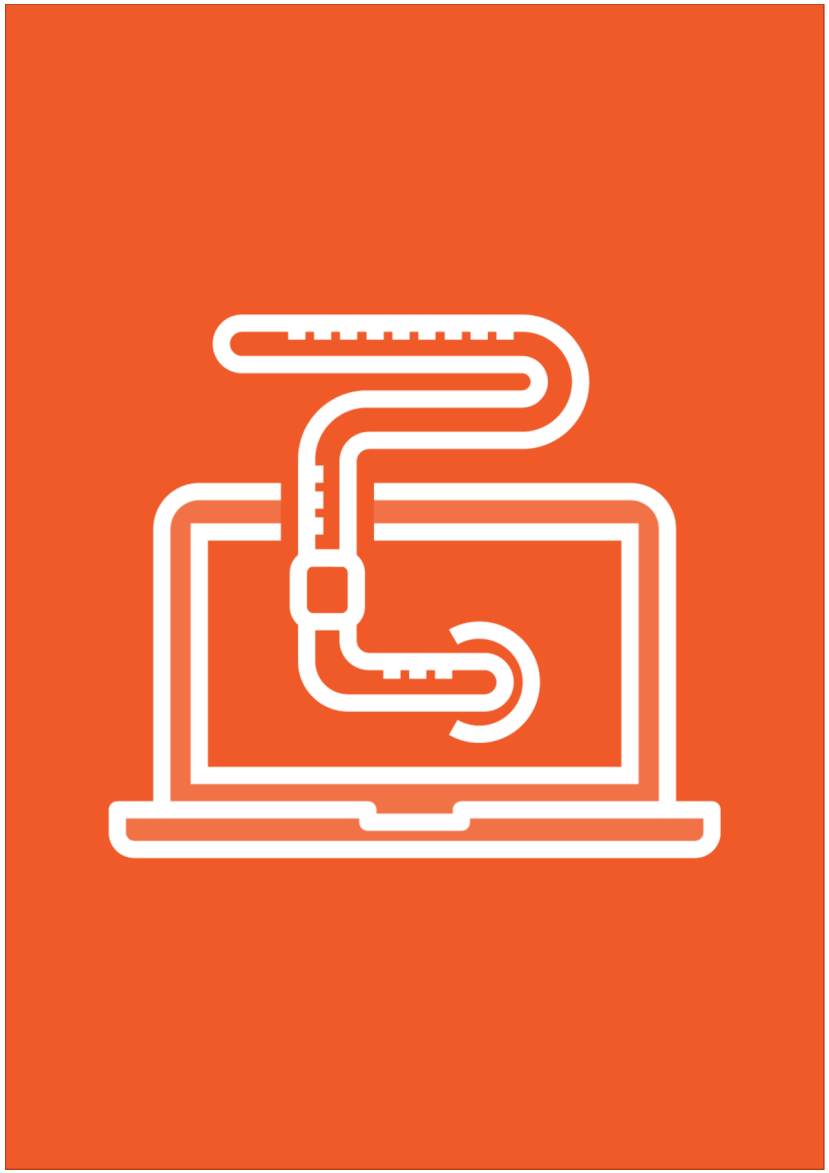


Passive

Active



No direct interaction with the target



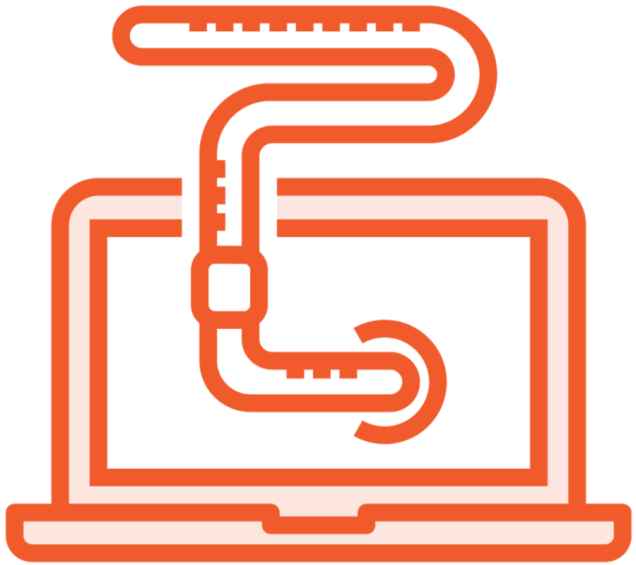
No direct interaction with the target

Research the company

Direct interaction with the target

Direct interaction with the target

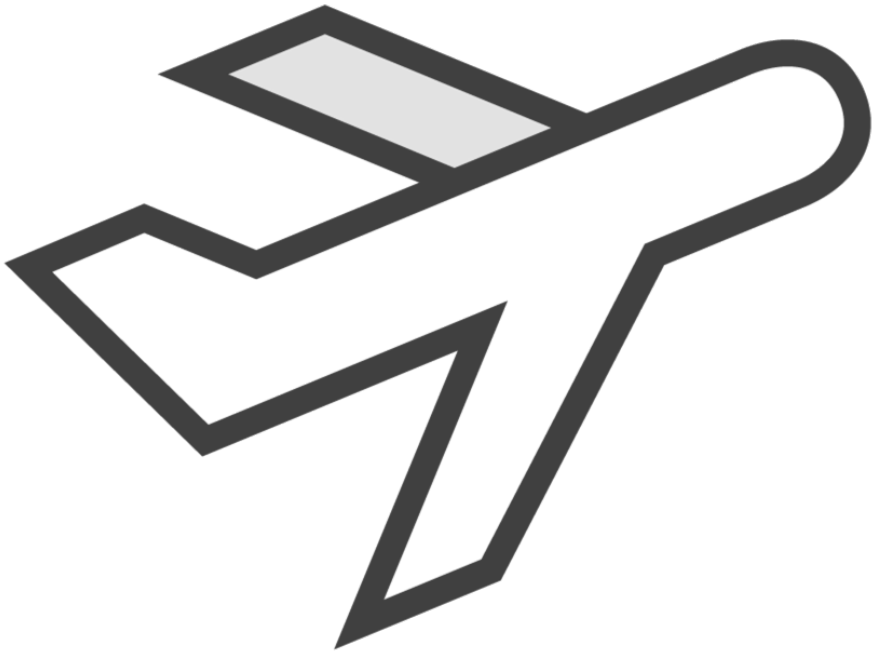
Engage and scans the network



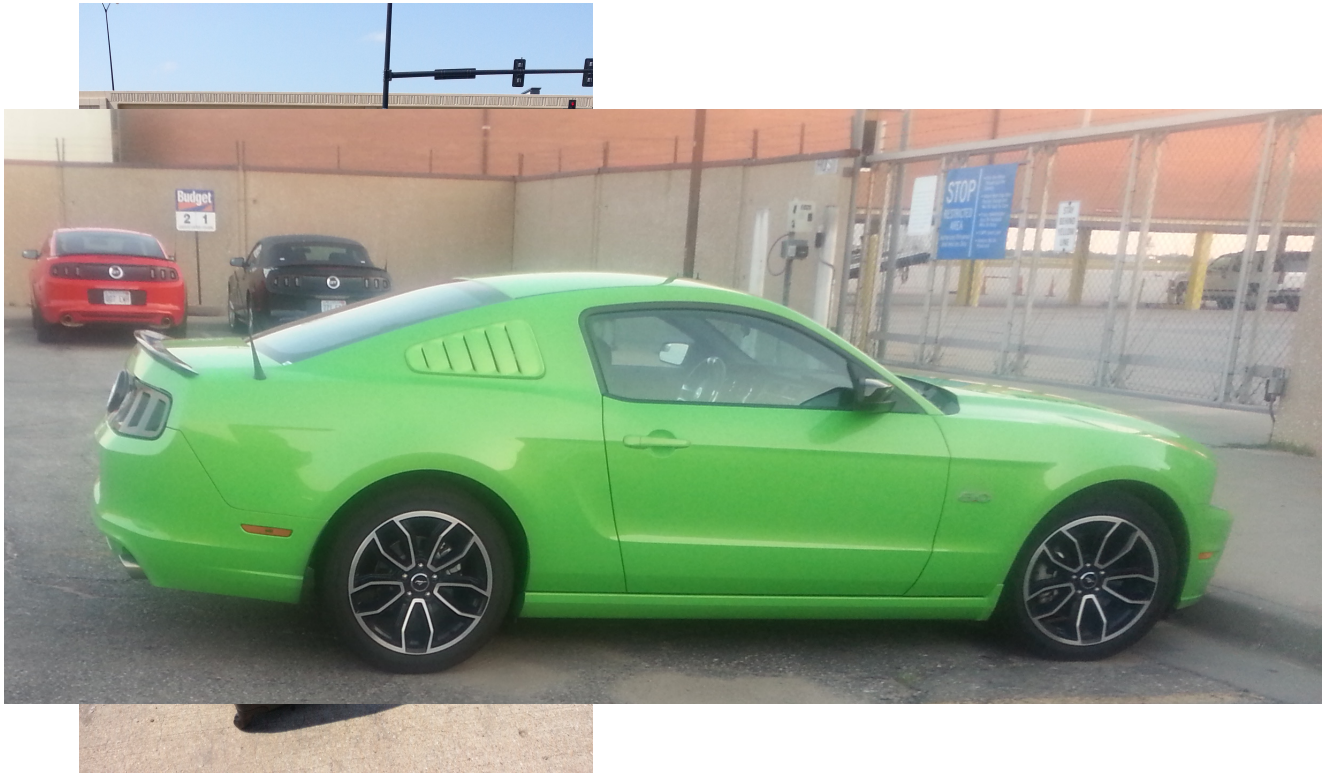
Social Engineering

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

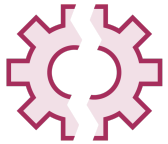
Via OS

Via application

What is the goal?

Goals

Access data

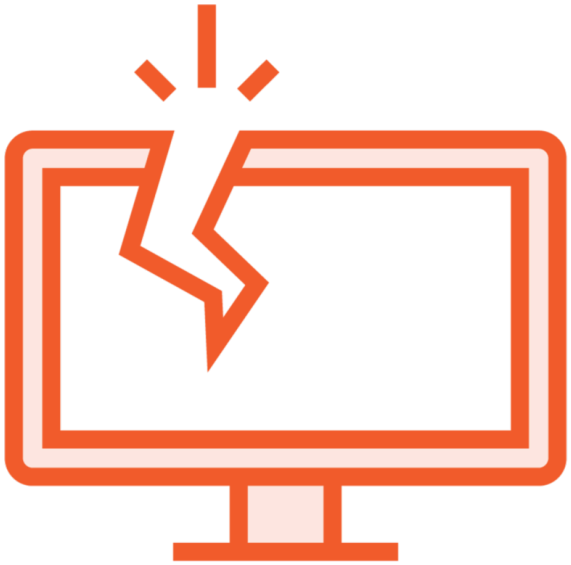


Reconfigure or crash a system

Exhaust the resources

Password cracking | Buffer overflows | Session hijacking | Denial of service

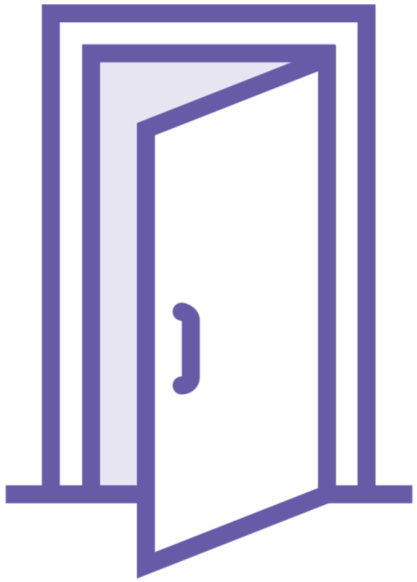
in



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?

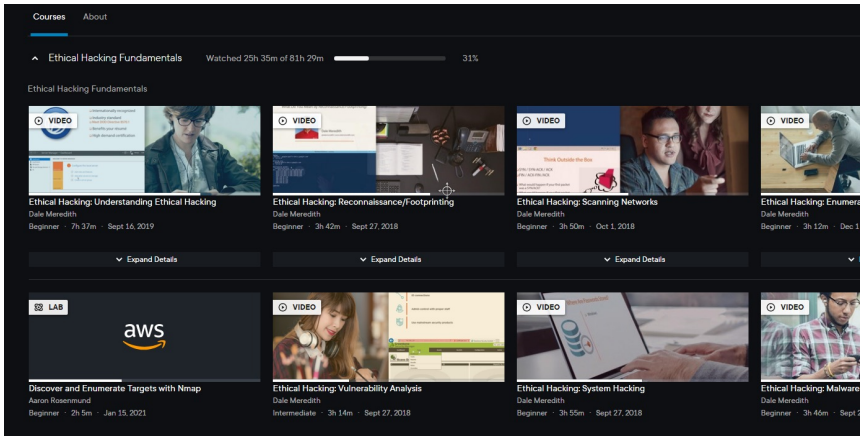
Involves the use of hacking methods and tools to discover weaknesses for system security

What Skills Should an Ethical Hacker Have?

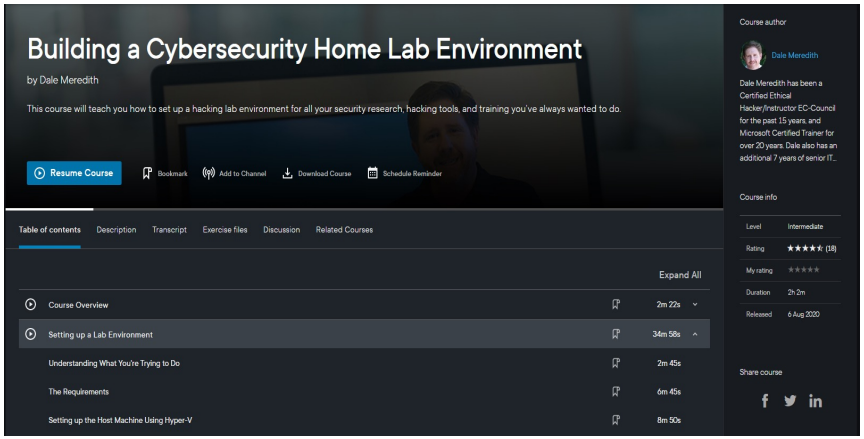
- Expert with programs and networks
- Proficient with vulnerability research
- Mastery with diverse hacking techniques
- Follow a strict code of conduct
- Explicit permissions in writing
- Use the same tactics and strategies
- Just because you can, doesn't mean you can
- Report all of your results

Let's Talk About the Labs

Let's Talk About the Labs



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