

Hacking Phases



Dale Meredith

@dalemeredith | www.daledumbsitdown.com

What is the *MOST* secure
system?

The one that is never built

You Can't Stop "Them"



Your job is to discourage, misdirect and
slow them down

You Can't Stop "Them"



Time is NOT on your side

You Can't Stop "Them"



Attacker only has to find 1 opening
You have to cover all of them

The Phases

Reconnaissance

Scanning

Gaining access

Maintaining
access

Clearing tracks

Phase 1) Reconnaissance



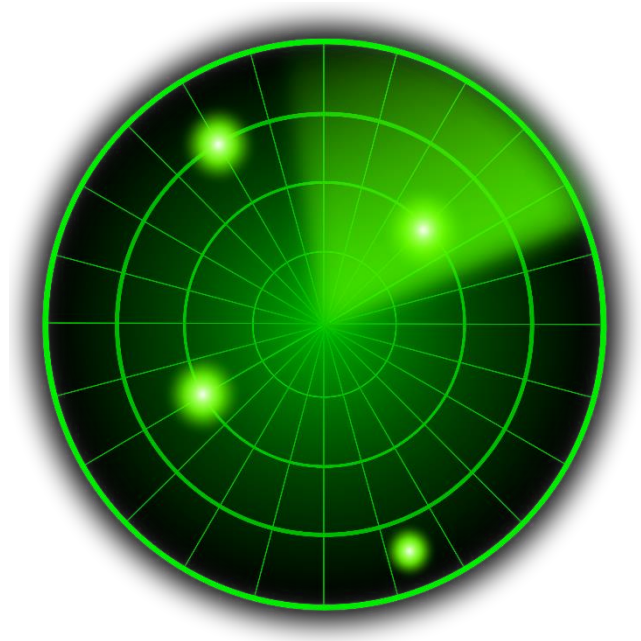
Passive

- No direct interaction with the target

Active

- Direct interaction with the target

Phase 2) Scanning



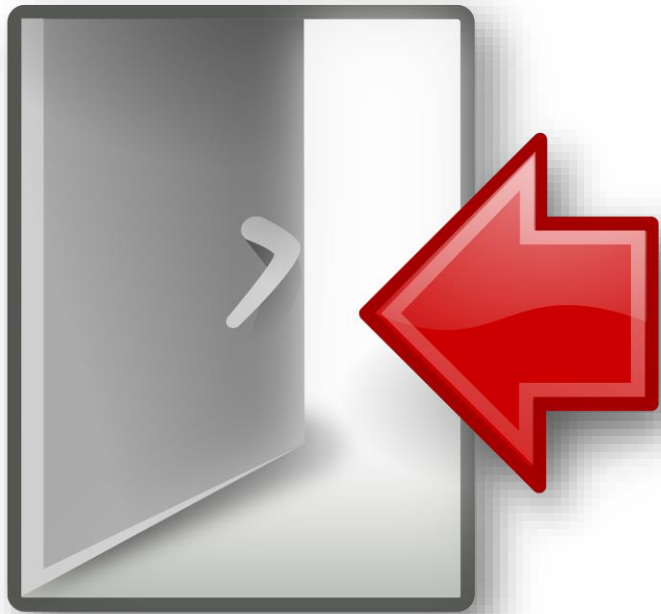
Gather Info

- ID systems
- Vulnerabilities

Tools Used

- Port Scanners
- Vulnerability Scanners

Phase 3) Gaining Access

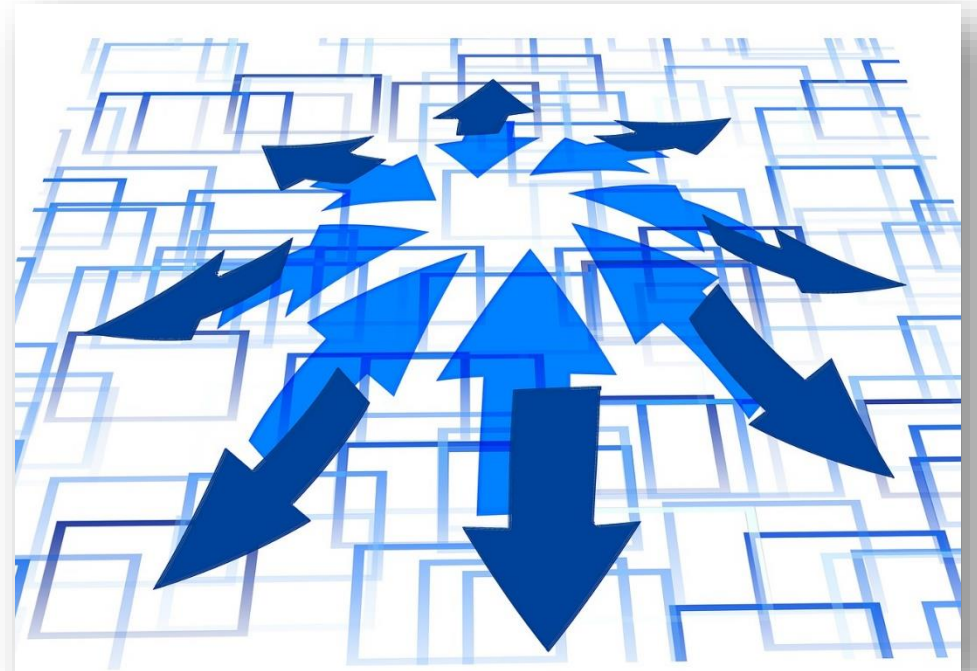


Path

- ❑ Via network
- ❑ Via OS
- ❑ Via application
- ❑ Our goal?
 - ❖ To escalate privileges

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



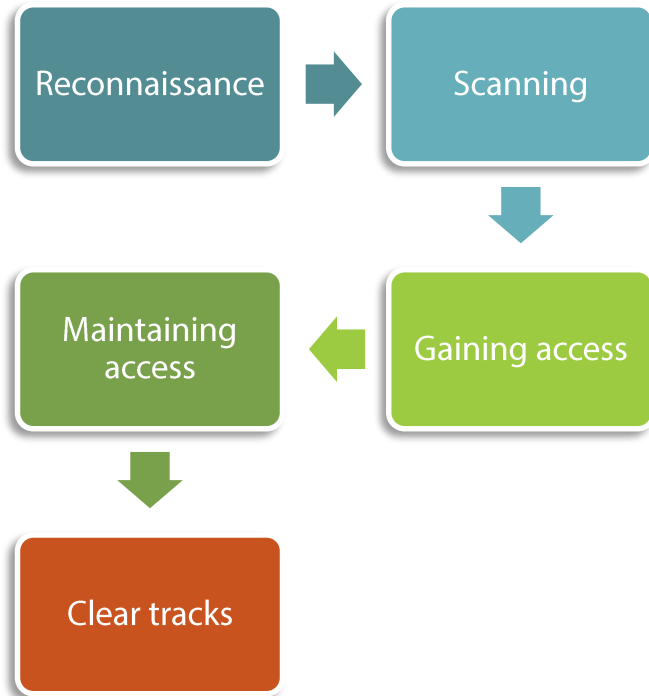
Phase 5) Clearing Tracks



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

- ❑ Destroy proof
- ❑ Hide my stuff
- ❑ Cyber blind

Summary



- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clear tracks