Defining Penetration Testing

Module Overview

Penetration testing

Passive and active reconnaissance

Exercise types

Module Overview

- Penetration testing
  - Known environment
  - Unknown environment
  - Partially known environment
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting
- Passive and Active Reconnaissance
  - Drones/unmanned aerial vehicle (UAV)
  - War flying
  - War driving
  - Footprinting
  - OSINT
- Exercise Types
  - Red team
  - Blue team
  - White team
  - Purple team

Penetration Testing

Also called pen testing, is the practice of testing a computer system, network or web application to find vulnerabilities that an attacker could exploit.

Steps of a Penetration Test

Establish Goal / Set Parameters

Reconnaissance / Discovery

Exploitation / Brute Force

Take Control / Escalate Privilege

Pivoting

Data Collection / Reporting

Remediate the Security Deficiencies!

Known, Unknown and Partially Known Environments

Unknown environment
Tester is given little to no information about the target. More like real world, but more time consuming and more expensive

Known environment
Tester is given full disclosure about the target (i.e. network, hosts, source code, protocols, diagrams, etc.)

Partially known
Combination of known and unknown, in that tester is given partial information about the target, but not access to documentation or data

Rules of Engagement

RoE should clearly define what is in-scope for the engagement

- What activities are allowed
- What activities are prohibited
- Key stakeholders
- Relevant contact lists
- Communication methods/frequency
- Handling of sensitive data
- Specific goals / definition of success

CREST Framework

Internationally recognized accreditation
Various areas of information security and assurance

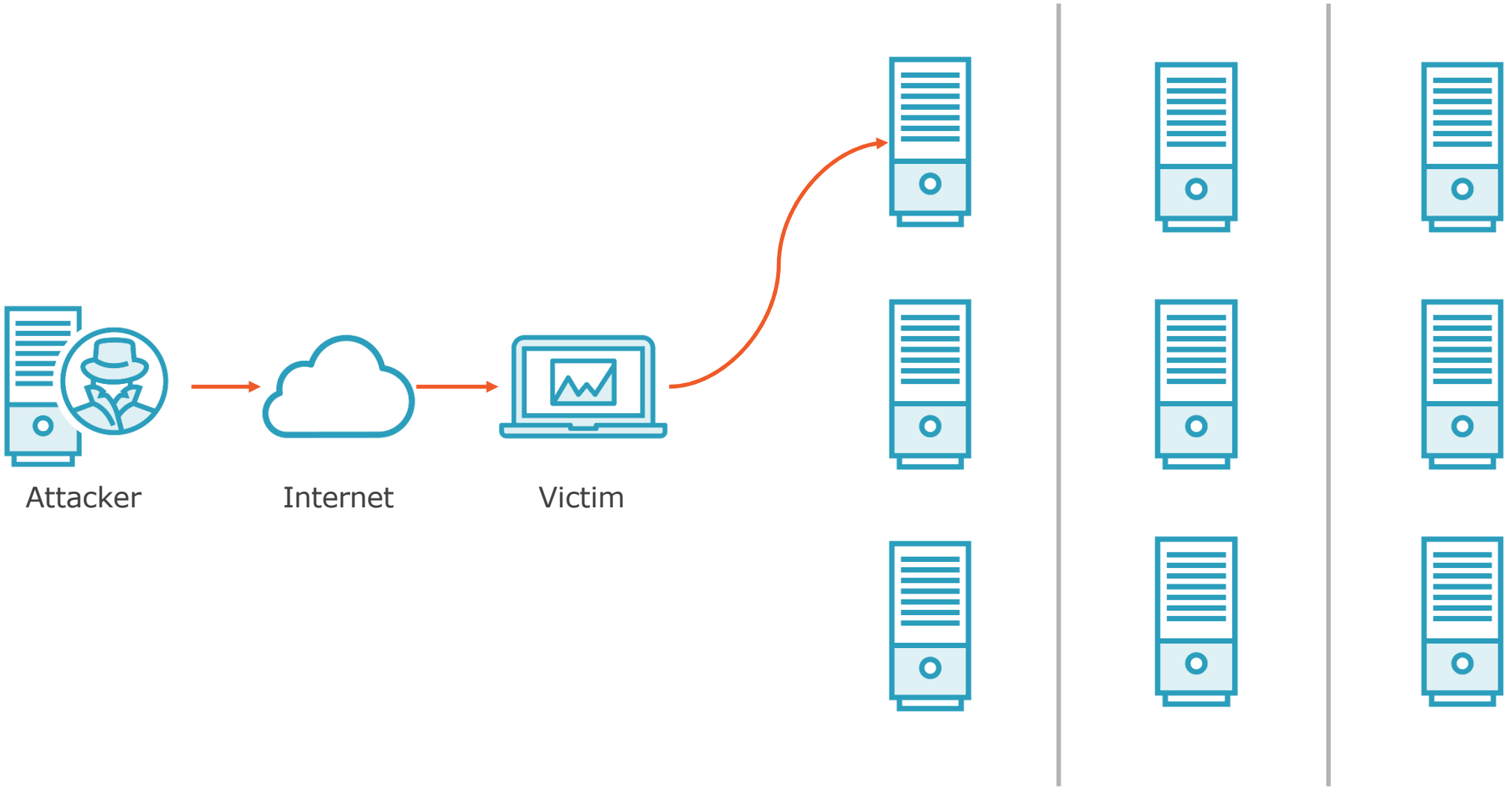
Provides vetted resources for companies looking for providers
Adherence to industry benchmarks and best practices

Government and regulatory standardization
Access to qualified talent, supply chain and logistics assurance

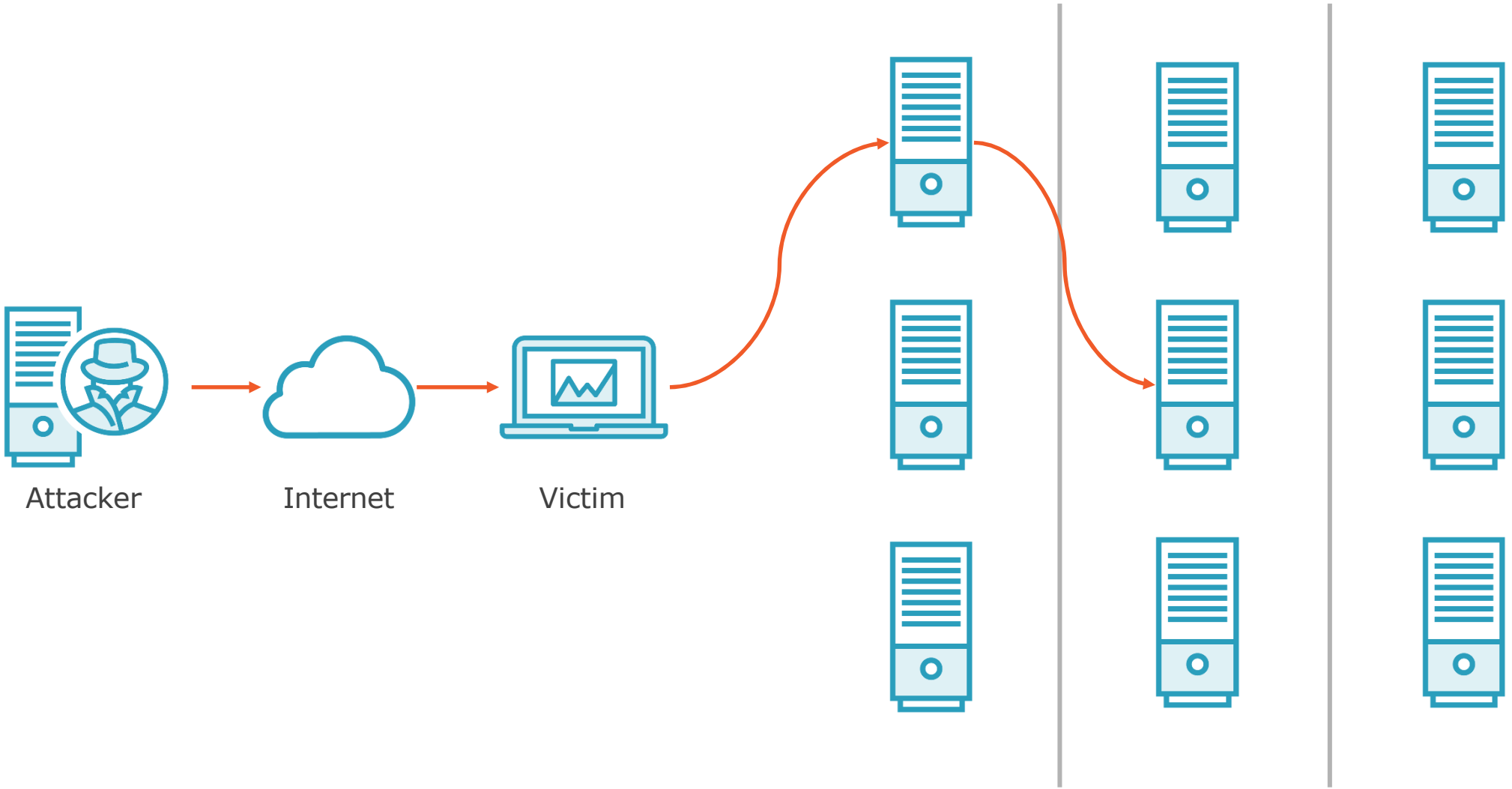
https://crest-approved.org

Lateral Movement

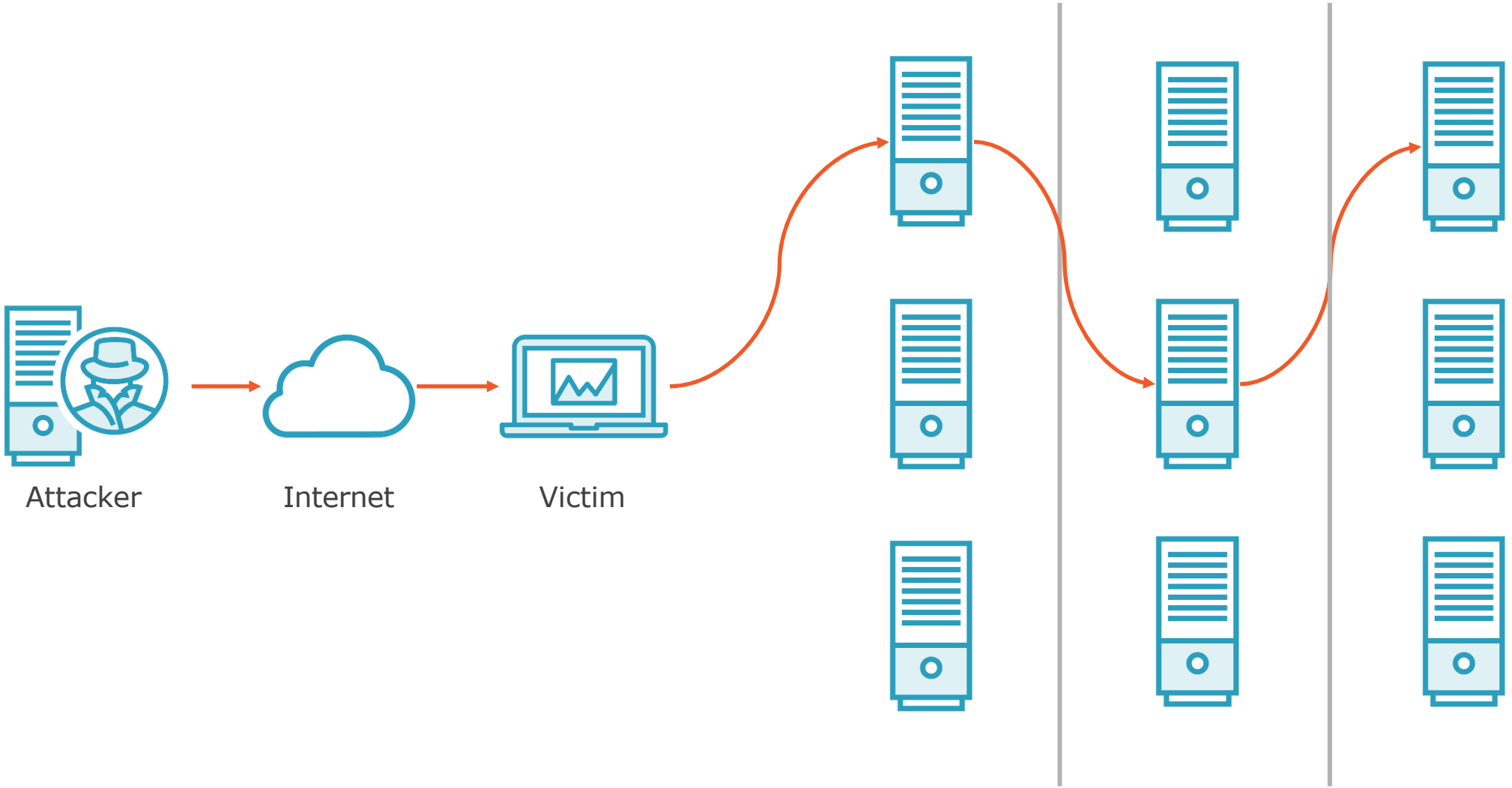
Lateral Movement



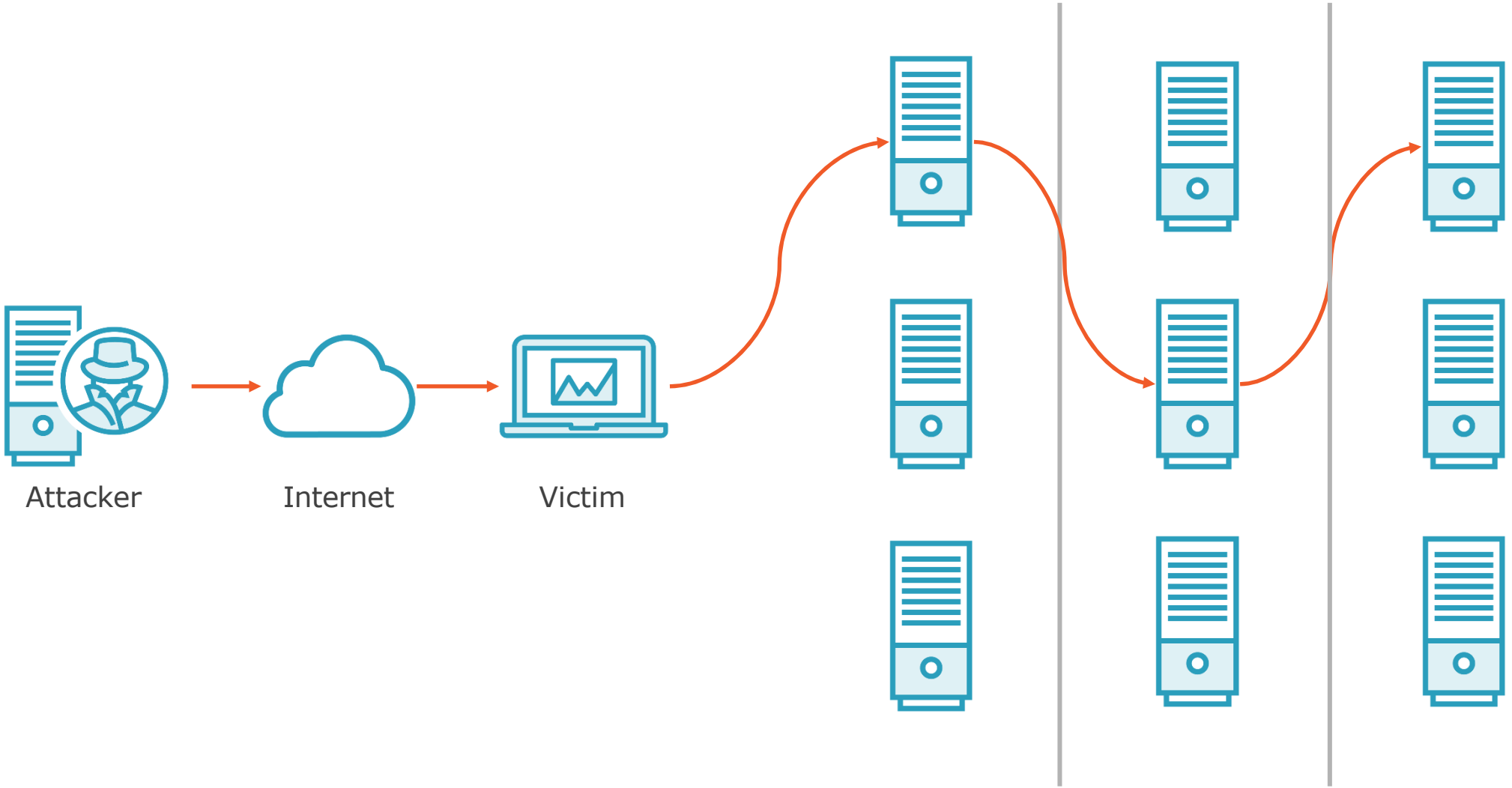
Lateral Movement



Lateral Movement



Lateral Movement



Escalation of Privilege

Primary goal when accessing a host

- Administrator or Root access to the host
- Enables installation of persistence mechanisms
- Scan for additional exploits, vulnerabilities and misconfigurations

Methods of Privilege Escalation

Hack the local admin account

Exploit a vulnerability

Use tools / brute force

Social engineering

Persistence

Installing backdoors or methods to maintain access to a host or network

Cleanup

Removing traces of the attack

- Removing files
- Cleaning/deleting log files
- Intentionally leaving false artifacts
- Encrypting or deleting data

Firewalls, routers, servers

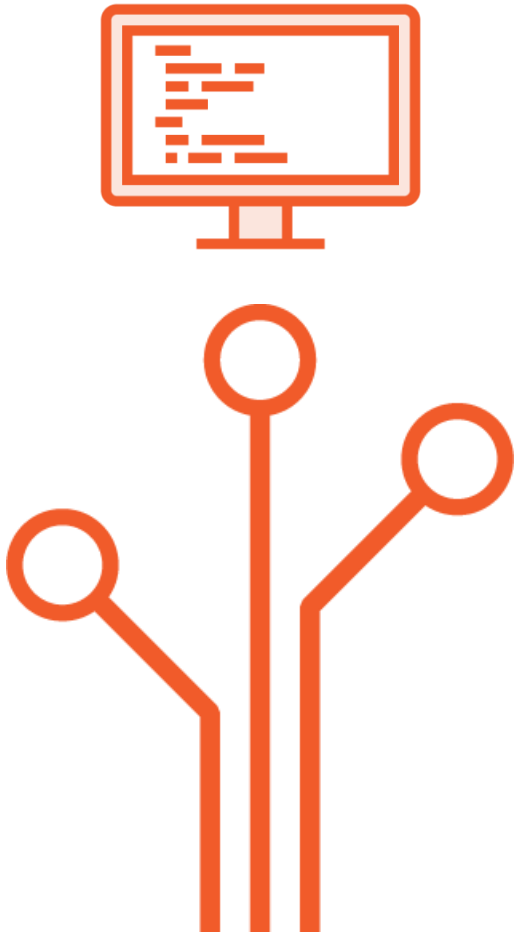
Bug bounty

- Program to encourage users to find and report bugs
  - Awards range from recognition to compensation
- First known bug bounty was implemented in 1983
- Netscape engineer coined the phrase in 1995

Bug bounty programs

- Hackerone.com offers bug bounty programs with a network of over 750k ethical hackers

Pivoting



Pivoting is a technique that allows lateral movement from a compromised host

- Foothold is gained on a target system
- Compromised target system is leveraged to compromise other, normally inaccessible systems

Many tools (i.e. Metasploit) have built in utilities to automate much of the process

Pivoting

Types of Reconnaissance

Passive Reconnaissance

Utilize publicly accessible methods to discover information about the target

No direct contact with the target company

Public records

Google searches / GHDB

Company website / Wayback machine

Active Reconnaissance

Direct access to the target company

Asking questions of employees, management, etc

Entering the facilities and walking the site

Seeing where you can go, what things you can access

Active scanning/fingerprinting the network, hosts, etc

War Flying

- Using and airplane, drones or UAV to sniff Wi-Fi networks
  - Calculate GPS coordinates,
  - Aerial imagery
- Typical flight times can last up to 30-45 minutes
- Drones have been shown to pick up networks even at elevations of 1,500 to 2,000 feet

War Driving

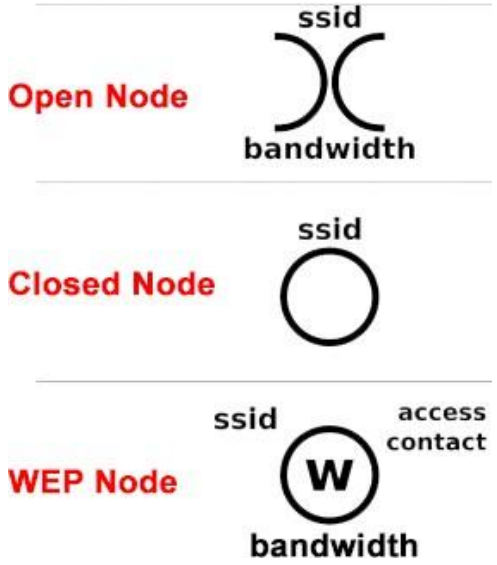
Actively seeking out wireless access points with little to no security

- Open, WEP, WPA

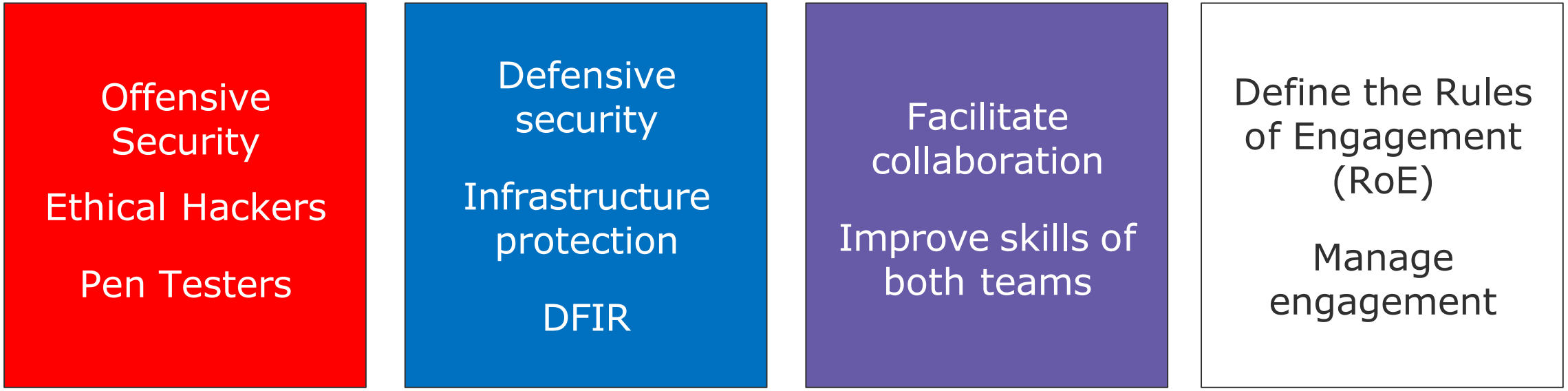
War Driving


ScanBox
powered by
Cyanitic


RINGLES
Pringles


Open Node
ssid
bandwidth
Closed Node
ssid
WEP Node
ssid
access
contact
W
bandwidth

Security Teams



Red Team
(Attackers)

Blue Team
(Defenders)

Purple Team
(Collaborators)

White Team
(Managers)

Fully Document and Report

Once the exercise is over, fully document and report back to executive management

Module Review

Penetration testing

Passive and active reconnaissance

Exercise types