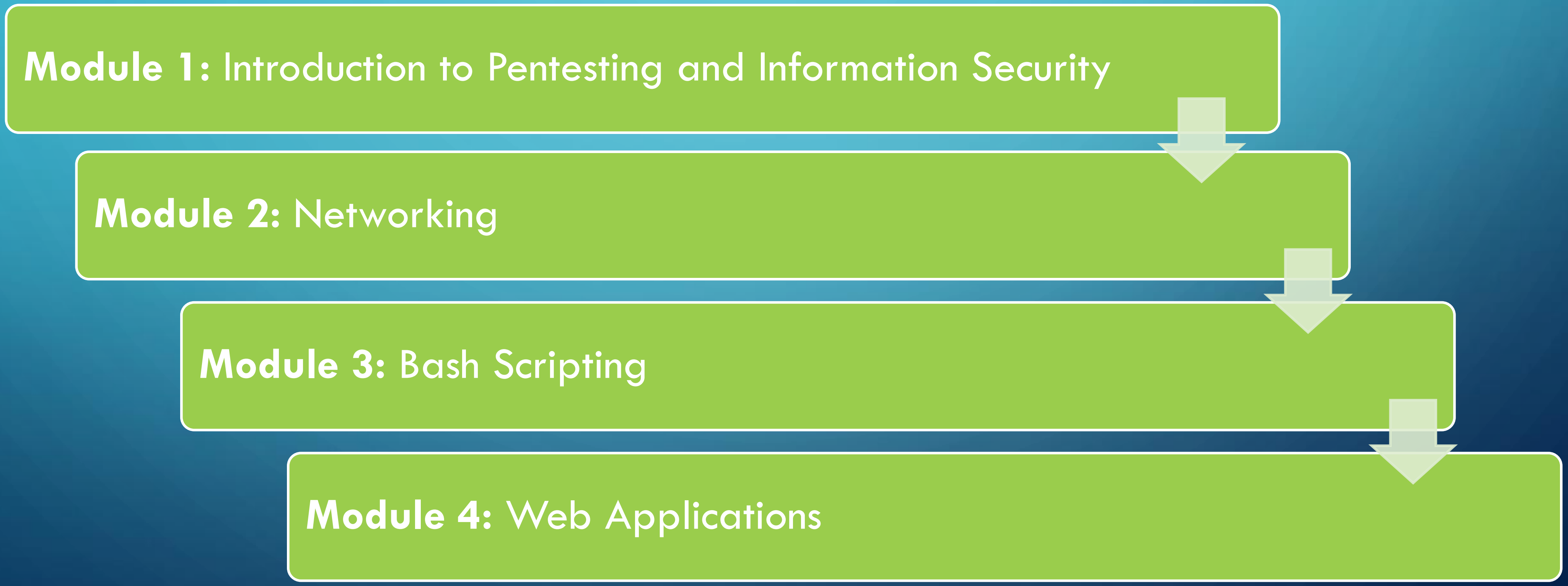
C.F.A

Penetration Testing Course Content

PRELIMINARY SKILLS - (PREREQUISITES & PROGRAMMING)



Module 1: Introduction to Pentesting and Information Security

Module 2: Networking

Module 3: Bash Scripting

Module 4: Web Applications

Module 1: Introduction to Pentesting and Information Security

- Introduction to Information Security
- Information Security Attacks and Information Security Controls
- Hacking Concepts
- Introduction to Penetration Testing
- Lifecycle of a Penetration Test
- Engagement, Information Gathering, Footprinting and Scanning, Vulnerability Assessment,
- Exploitation and Reporting.
- Examples of the Vulnerability
- Red Team && Blue Team
- Capture The Flag (CTF)

Module 2: Networking

- Network
- Types Of Network
- Network Topologies
- The 7 Layers Of The OSI Model
- Layer 7 - Application
- Layer 6 - Presentation
- Layer 5 - Session
- Layer 4 - Transport
- Layer 3 - Network
- Layer 2 - Data Link
- Layer 1 - Physical

C.F.A

Module 3: Bash Scripting

Introduction to Bash

Linux commands

Linux File Permissions

Programming using Bash

Variables and Read from user

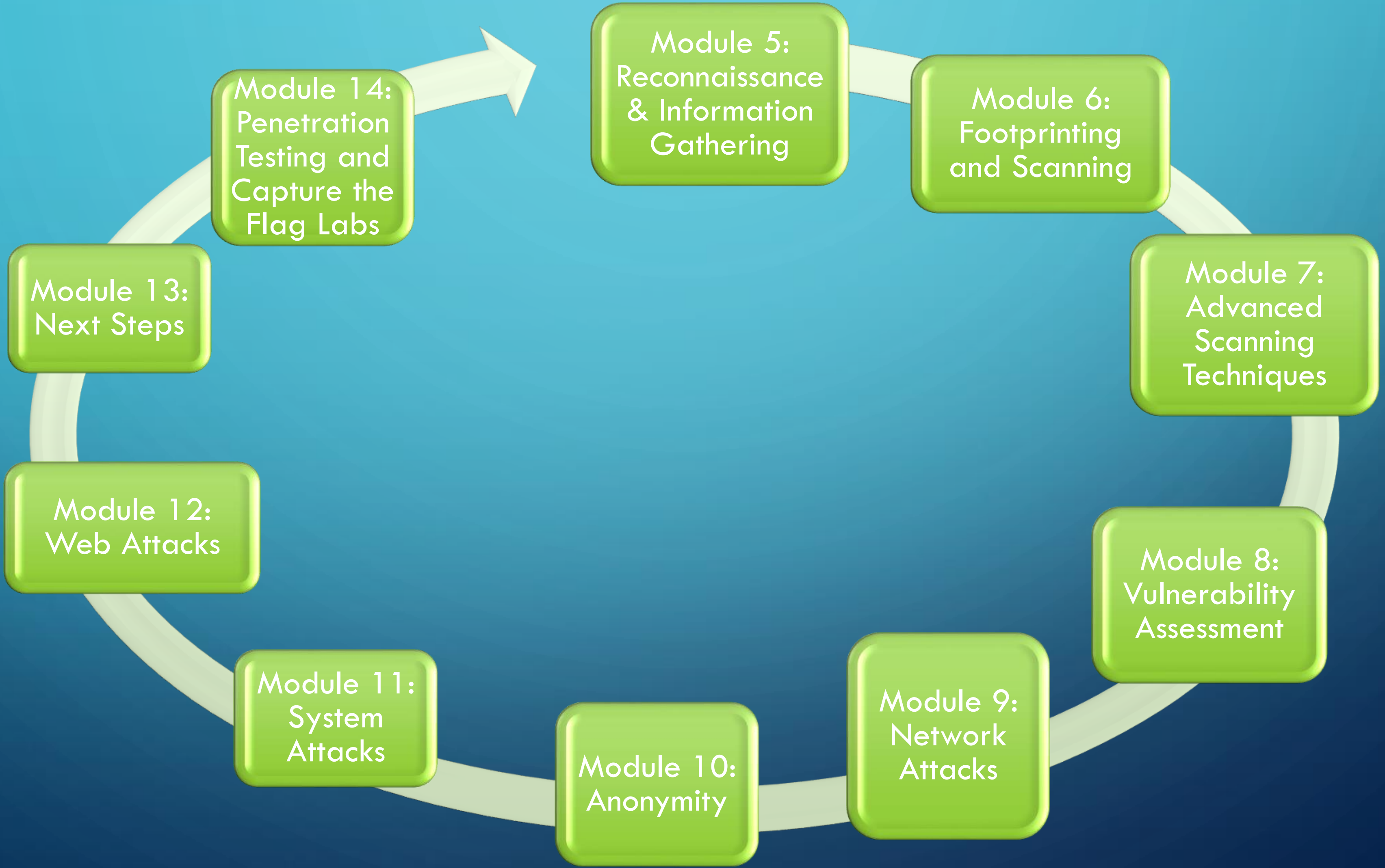
Shell Programming - Arithmetic Operators

Module 4: Web Applications

- Introduction
- HTTP Protocol Basics
- HTTP Cookies
- Sessions
- Same Origin Policy
- Burp Suite

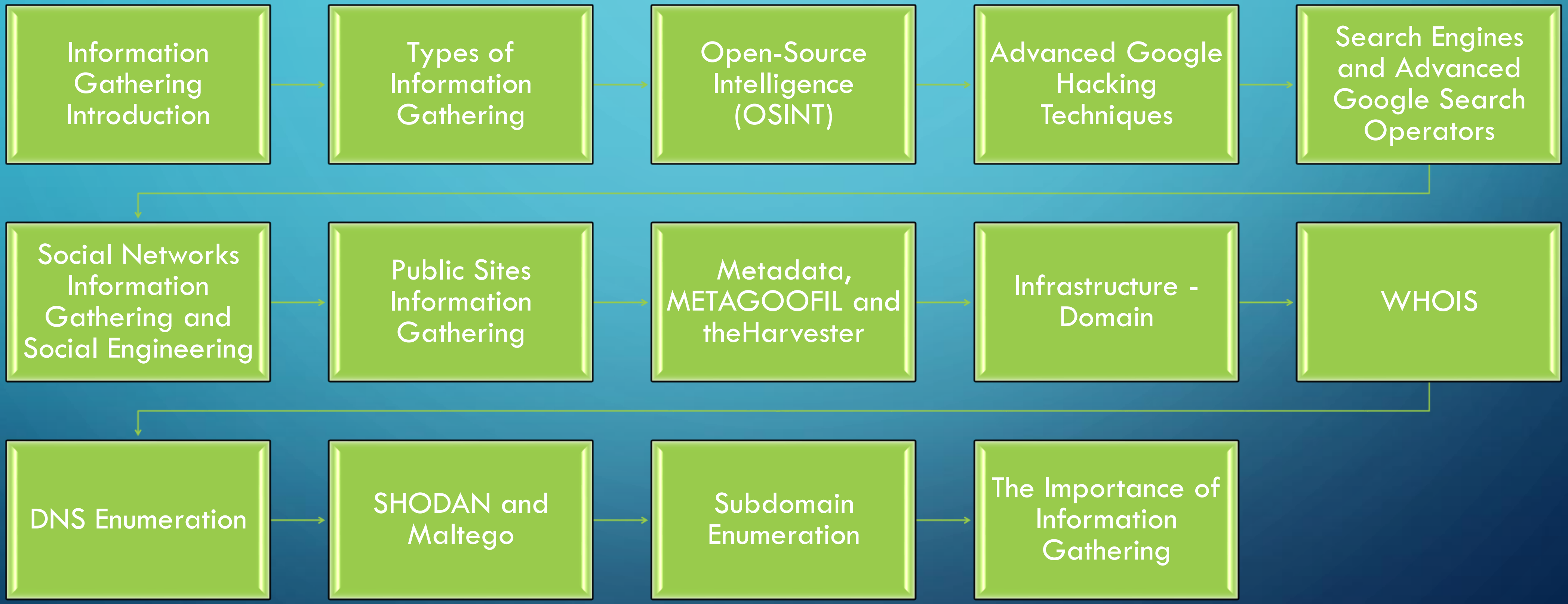
C.F.A

PENETRATION TESTING


Module 5: Reconnaissance & Information Gathering
Module 6: Footprinting and Scanning
Module 7: Advanced Scanning Techniques
Module 8: Vulnerability Assessment
Module 9: Network Attacks
Module 10: Anonymity
Module 11: System Attacks
Module 12: Web Attacks
Module 13: Next Steps
Module 14: Penetration Testing and Capture the Flag Labs

C.F.A

Module 5: Reconnaissance & Information Gathering



Information Gathering Introduction

Types of Information Gathering

Open-Source Intelligence (OSINT)

Advanced Google Hacking Techniques

Search Engines and Advanced Google Search Operators

Social Networks Information Gathering and Social Engineering

Public Sites Information Gathering

Metadata, METAGOOFIL and theHarvester

Infrastructure - Domain

WHOIS

DNS Enumeration

SHODAN and Maltego

Subdomain Enumeration

The Importance of Information Gathering

C.F.A

Module 6: Footprinting and Scanning

- Network Discovery and Mapping
- Scanning Goals and Types
- Mapping a Network
- Why Map a (Remote) Network
- Network sweeping
- Ping Sweeping
- Nmap Ping Scan
- Network Fingerprint
- Possibly identify operating system
- Active Fingerprinting - Passive Fingerprinting
- Network Scanning
- Port Scanning (TCP Port Scanning - UDP Port Scanning)
- Services Scanning (Nmap - Metasploit - Netcat)

Module 7: Advanced Scanning Techniques

- Wireshark for the Pen Tester
- Firewall / IDS Evasion Techniques
- Timing Options
- Bypass by Fragment Packets
- Bypass Firewall by Specify a Specific MTU
- Bypass by Decoys
- Bypass by Source Port Number Specification
- Bypass by Append Random Data
- Bypass by Send Bad Checksums
- Bypass by Idle Zombie Scan

Module 8: Vulnerability Assessment

- Vulnerability Assessment
- Vulnerability Scanners
- Manual Testing
- Nessus
- OpenVAS
- NMAP Scripting Engine
- Under the Hood of a Vulnerability Scanner
- Port Scanning
- Service Detection
- Vulnerabilities Database Lookup

Module 9: Network Attacks
9.1 Authentication Cracking

Brute Force vs. Dictionary Attacks

Weak and Default Credentials

Installing Dictionaries

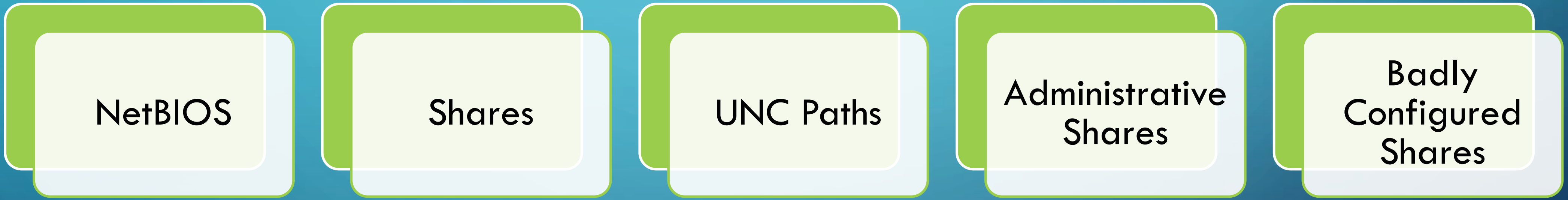
Authentication Cracking Tools

Hydra

Telnet Attack Example

HTTP Basic Auth Attack Example

Module 9: Network Attacks
9.2 Windows Shares



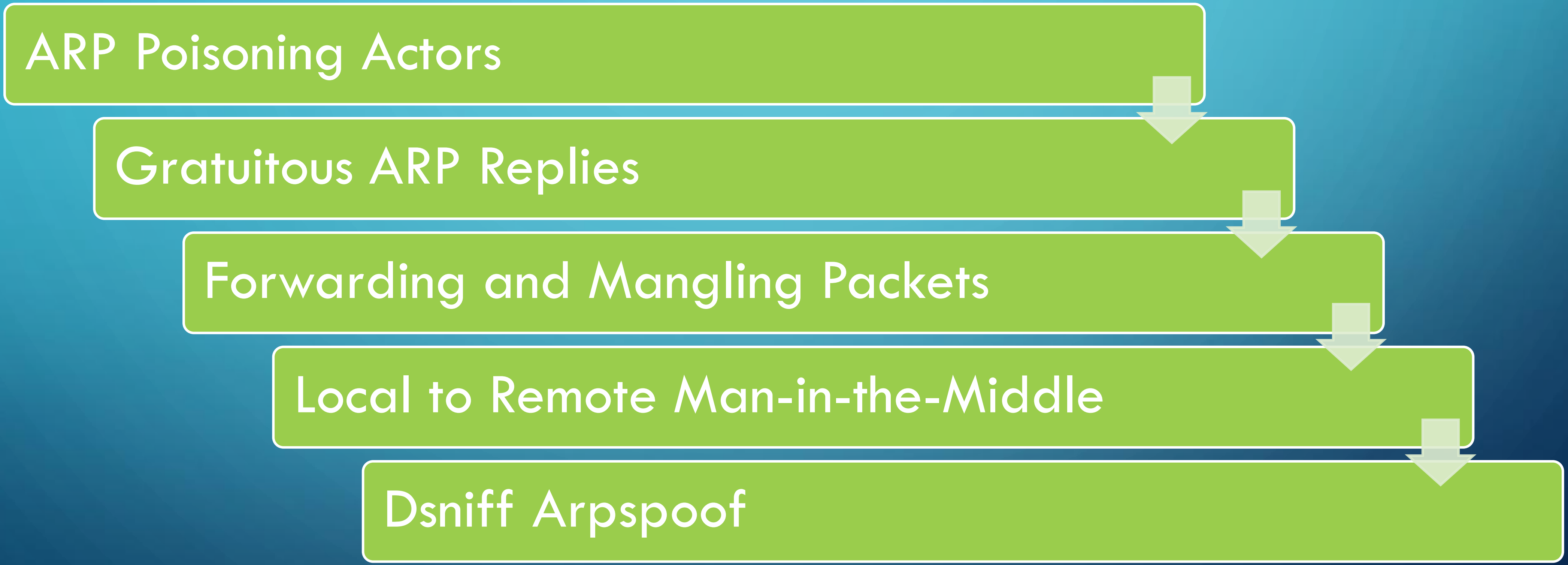
- NetBIOS
- Shares
- UNC Paths
- Administrative Shares
- Badly Configured Shares

Module 9: Network Attacks

9.3 Null Sessions

1. Enumerating Windows Shares
2. Checking for Null Sessions
3. Checking for Null Sessions with Windows
4. Checking for Null Sessions with Linux
5. Exploiting Null Sessions

Module 9: Network Attacks
9.4 ARP Poisoning



ARP Poisoning Actors

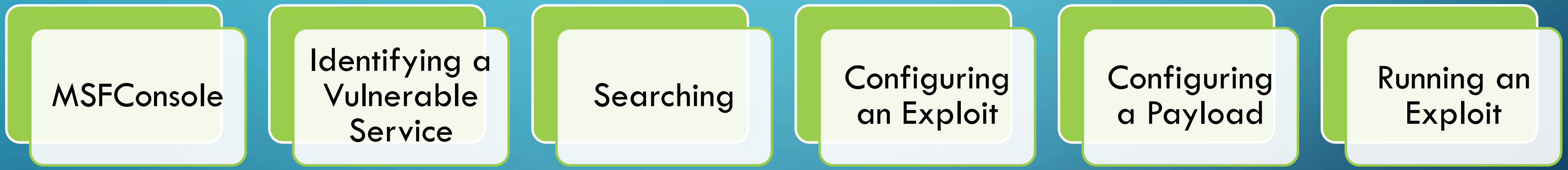
Gratuitous ARP Replies

Forwarding and Mangling Packets

Local to Remote Man-in-the-Middle

Dsniff Arpspoof

Module 9: Network Attacks
9.5 Metasploit



MSFConsole

Identifying a Vulnerable Service

Searching

Configuring an Exploit

Configuring a Payload

Running an Exploit

Module 9: Network Attacks
9.6 Meterpreter

- Bind and Reverse
- Launching Meterpreter
- Sessions
- Information Gathering with Meterpreter
- System Information
- Network Configuration
- Routing Information
- Current User

Module 9: Network Attacks
9.7 Privilege Escalation

1 Bypassing UAC

2 Dumping the Password Database

3 Exploring the Victim System

4 Uploading and Downloading files

5 Running an OS Shell

Module 9: Network Attacks
9.8 Antivirus Evasion

Module 10: Anonymity

Using of Anonymity During Testing of Networks

Browsing Anonymously

HTTP Proxies

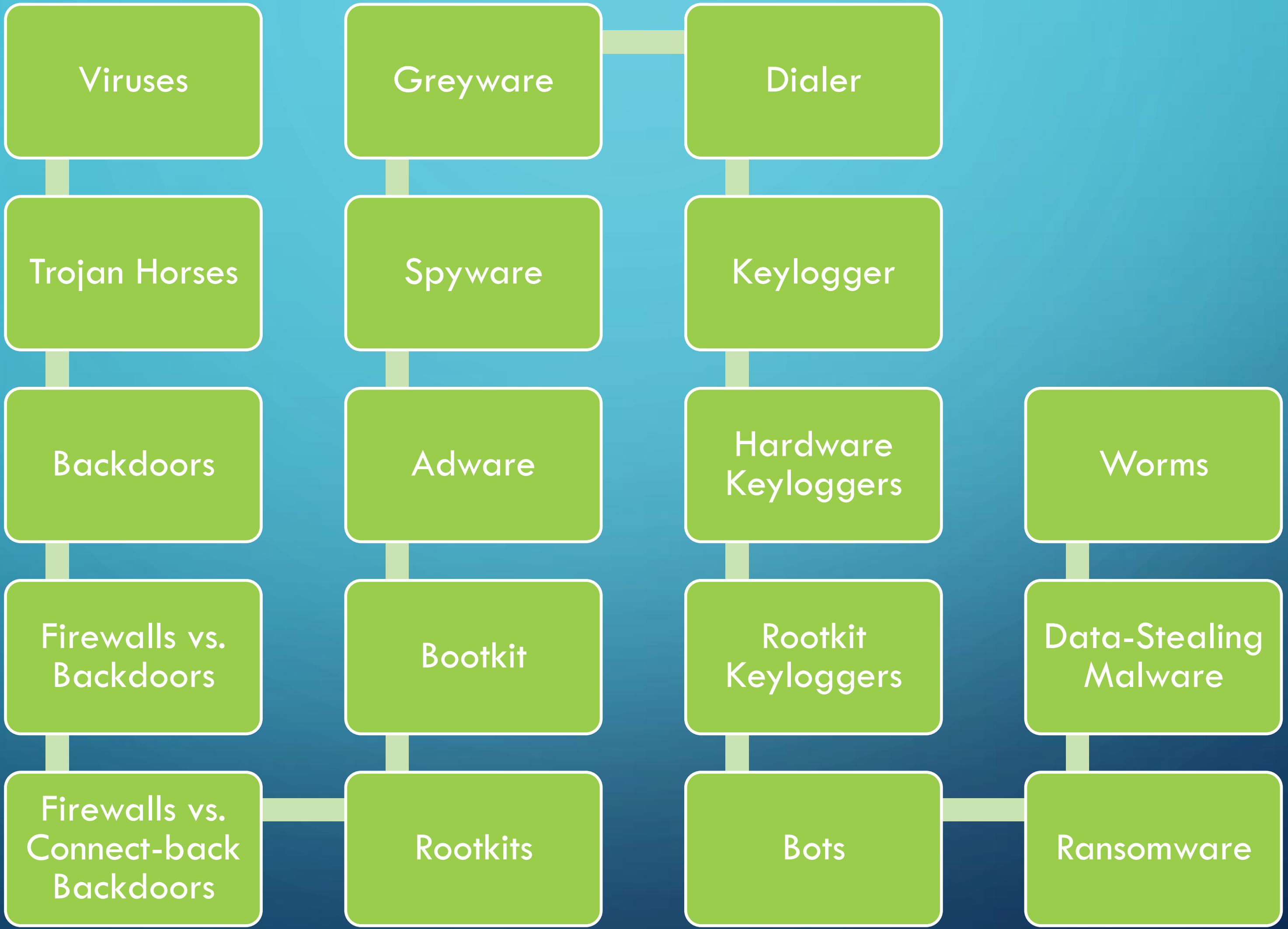
ProxyChains

Tunneling for Anonymity

SSH Tunneling

C.F.A

Module 11: System Attacks
11.1 Malware



Viruses

Trojan Horses

Backdoors

Firewalls vs. Backdoors

Firewalls vs. Connect-back Backdoors

Rootkits

Bootkit

Adware

Spyware

Greyware

Dialer

Keylogger

Hardware Keyloggers

Rootkit Keyloggers

Bots

Ransomware

Data-Stealing Malware

Worms

Module 11: System Attacks
11.2 Password Attacks

- Cryptography
- Types of Cryptography
- Password Attacks
- Dictionary Attacks
- Installing Password Dictionaries
- Brute Force Attacks and Algorithm
- Crack Hash By John The Ripper
- Hash-Identifier
- Hash Type is used by GNU/Linux and Windows
- Crack Linux Hash and Windows Hash By John The Ripper
- Rainbow Tables
- Ophcrack Tool to Crack Hash Windows
- Network Service Attack By Hydra Tool
- Pass The Hash Attack

Module 11: System Attacks
11.3 Buffer Overflow

- How to Hack any Application in the World ?
- Understand the Computer Working
- Stack Buffer Overflow
- Buffer Overflow Attacks
- Buffer Overflow Example
- How Buffer Overflow Attacks Work

C.F.A

Module 12: Web Attacks

- Introduction
- Web Server Fingerprinting
- HTTP Verbs
- Directories and File Enumeration
- Google Hacking
- Cross-Site Scripting
- SQL Injections

Module 13: Next Steps

- This module is a summary of the course. It contains useful advice and information about how to continue learning in the field of IT Security in the most efficient way. Also, students can test their skills against special lab challenges, which are very similar to real-life penetration testing scenarios.

Module 14: Penetration Testing and Capture the Flag Labs

C.F.A

Contact

Email :
cfaacademy21@gmail.com

Phone Number:
01090334063

Physical Address:
Online

Course duration:
80 hour