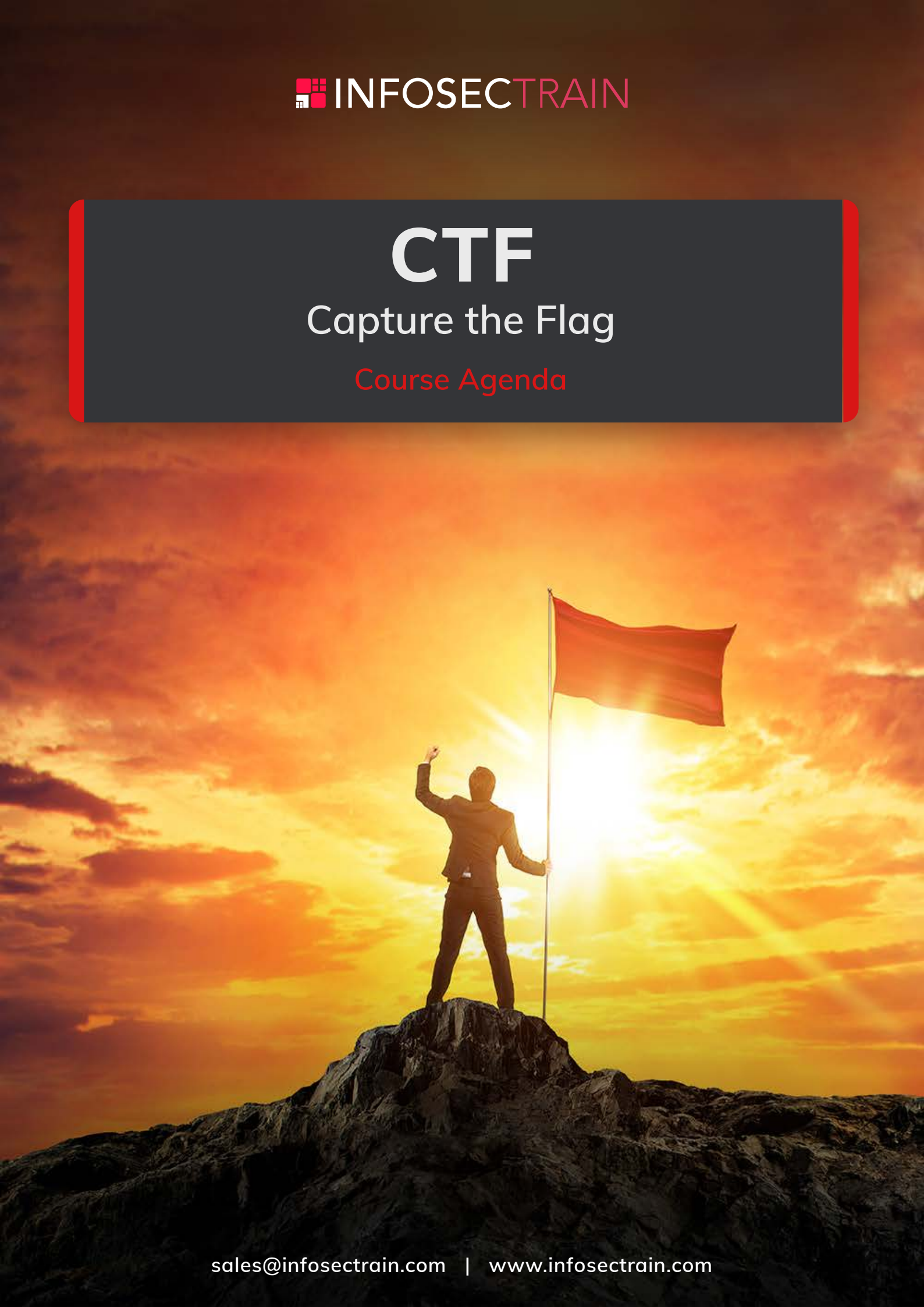
INFOSECTRAIN

CTF

Capture the Flag

Course Agenda



sales@infosectrain.com | www.infosectrain.com

Course Objectives

- Introduction to Pentesting
- Assessment & Skill Management
- Basic Linux and Commands
- Netcat Tutorials
- Port Scanning with Nmap & WireShark
- Enumeration
- Passive Info Gathering
- Directory Bruteforce Attack
- Windows Security Assessment
- Reverse Shell
- Intro to Overflows
- Windows BO Example
- Linux BO Example
- Using Public Exploits
- File Transfers
- Linux Privilege Escalation
- Windows Privilege Escalation
- Web Application Attacks
- Password Cracking
- Port Fun
- Metasploit Framework
- Antivirus Avoidance
- Misconfigured Lab Setup

Introduction to Pentesting

- Penetration Testing Benefits
- Types of Penetration Testing
- Penetration Testing Methodologies
- Law & Compliance
- Planning, Managing & Reporting

Assessment & Skill Management

- ssessment & Skill Management
- Finding Files
- Services in Kali
- SSH Service
- FTP Services
- HTTP Service
- SNMP Service
- Mysql Services
- Service Management
- IP Protocols, Networking Protocols, IPSec, VOIP
- Network Architecture, Mapping & Target Identification

Basic Linux and Commands

- Locate
- Which
- Find
- Sed
- Awk
- Cut
- Sort
- Grep
- Head
- Tail
- Wget
- Cat

Netcat Tutorials

- Getting start with NC

- Connecting to a Server
- Fetching HTTP header
- Chatting
- Creating a Backdoor
- Verbose Mode
- Save Output to Disk
- Port Scanning
- TCP Delay Scan
- UDP Scan
- Reverse TCP Shell Exploitation
- Randomize Port
- File Transfer
- Reverse Netcat Shell Exploitation
- Banner grabbing

Port Scanning with Nmap & WireShark

- TCP Connect Scan with wireshark
- Network Sweeping with wireshark
- SYN Scan with wireshark
- UDP Scan with wireshark
- FIN Scan with wireshark
- Null Scan with wireshark
- OS Discovery with wireshark
- NSE Scripts with wireshark
- Nmap Firewall Scan

Enumeration

- Overview
- Structure, interpretation and analysis of DNS records
- DNS Enumeration

- Forward DNS Lookup
- Reverse DNS Lookup
- Zone Transfers
- NetBIOS & SMB Enumeration
- Null Sessions
- Enum4Linux
- SMB NSE Scripts
- MYSQL Enumeration
- MSSQL Enumeration
- SMTP Enumeration
- VRFY Script
- Python Port
- SNMP Enumeration
- SNMP MiB
- SNMPWalk

Passive Info Gathering

- Overview
- Google Search
- Google Hacking
- GHDB
- NNTP Newsgroups & Information Leakage from Mail Headers

Directory Bruteforce Attack

- Dirb
- Dirbuster
- Dirsearch
- Metasploit

Windows Security Assessment

- Domain Reconnaissance
- User Enumeration
- Active Directory
- Windows Patch Management Strategies
- Desktop Lockdown & Exchange Server

Reverse Shell

- Php reverse shell
- Python reverse shell
- Perl reverse shell
- Bash reverse shell
- Msfvenom shell

Intro to Overflows

- Overview
- Vulnerable Code
- Stack Overflow
- Heap Overrun/Overflow

Windows BO Example

- Overview DEP, ASLR and CFG
- Fuzzing
- Crash Replication
- Controlling EIP
- Locating space for our Shellcode
- Bad Characters
- Redirecting Execution
- Introducing Mona
- Shellcode Payload

Linux BO Example

- Overview DEP, ASLR and Canaries
- Controlling EIP
- Locating Space
- First Stage Shellcode

- Locating RET
- Generating Shellcode

Using Public Exploits

- Overview
- Finding Exploits
- Exploit-DB
- Fixing Exploits 1
- Fixing Exploits 2
- Cross-Compiling

File Transfers

- FTP
- Python HTTP Server
- php http server
- HFS Tool
- Netcat
- CURL
- Wget
- TFTP
- Python SMB Server
- Powershell File Transfer
- Bitsadmin

Linux Privilege Escalation

- Suid Binaries
- Absuing Sudo's Right
- Kernel Exploit
- Path Variables
- Multiple Ways to edit /etc/passwd file

Windows Privilege Escalation

- Weak File Permissions
- Always Install Elevated
- Bypass UAC

- Unquoted Service Path
- Kernel Exploits

Web Application Attacks

- Overview
- Web Servers Flaws
- Web Protocols
- Local File Inclusion
- SQL Injection
- Authentication Bypass
- Error Based Enum
- Blind SQL Injection
- Attack Proxies
- XSS, LDAP & XML Injection
- SQLMap
- Web APIs
- Web Sub-Components

Password Cracking

- Overview
- Crunch
- Passing the Hash
- Password Profiling
- Online Attacks
- Medusa
- Ncrack
- Hydra
- Password Hashes
- Cracking Hashes
- LM / NTLM

Port Fun

- Overview
- Port Forwarding
- SSH Tunnels
- Dynamic Proxies
- Proxy Chains

Metasploit Framework

- Overview
- AUX Modules
- SNMP Modules
- SMB Modules
- WEBDAV Modules
- Database Services
- Exploits
- Payloads

- Meterpreter
- Meterpreter in Action
- Additional Payloads
- Binary Payloads
- Multihandler
- Porting Exploits
- Post Exploitation

Antivirus Avoidance

- Overview
- Shellter
- Veil-Evasion
- thefatrat

Misconfigured Lab Setup

- Wordpress lab Setup & Pentesting
- Joomla Lab Setup & Pentesting
- Drupal Lab Setup & Pentesting

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com