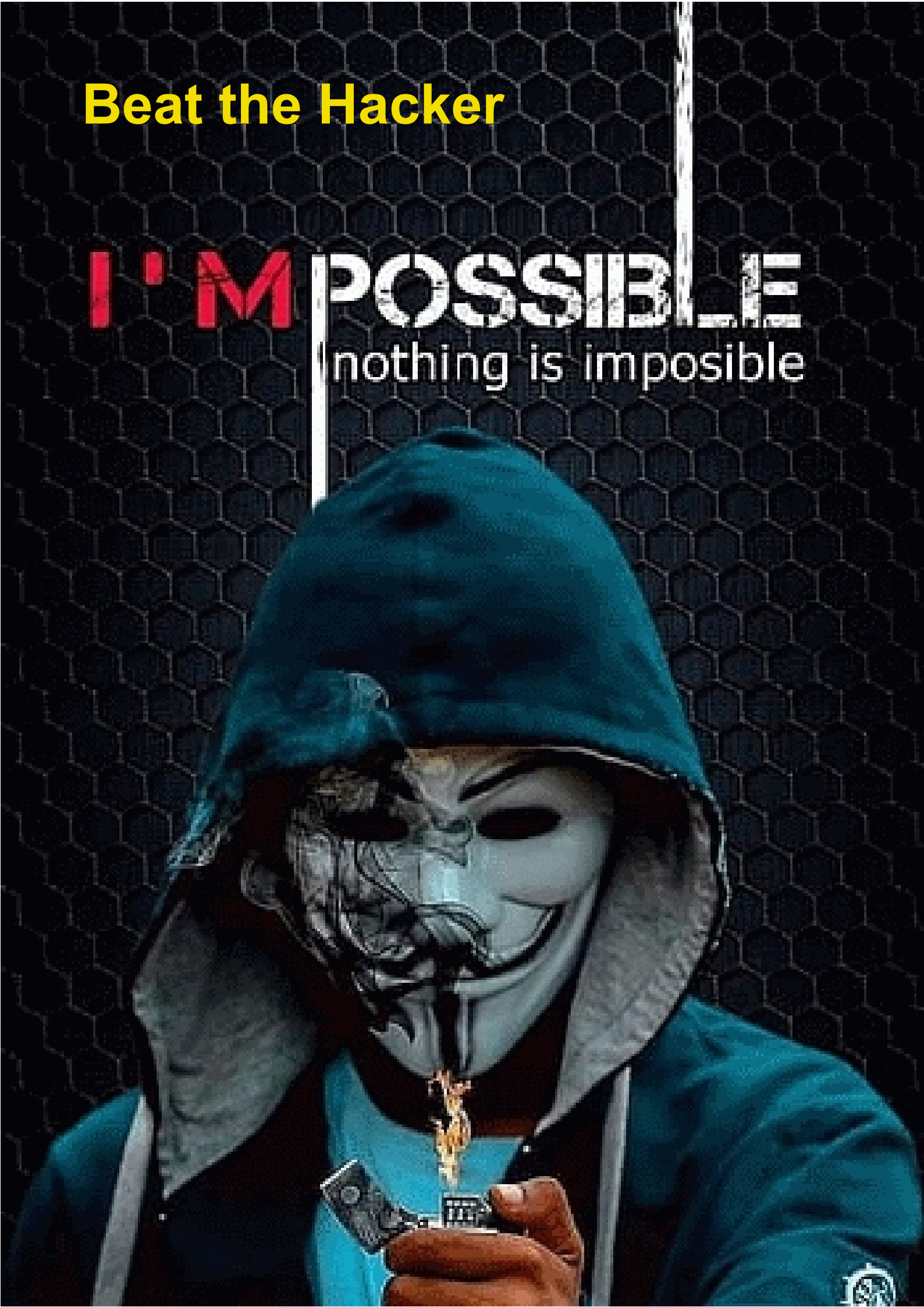
Technology Incubation Center CIU

Professional Certificate in Cyber Threat Hunting

Technology Incubation Center CIU

www.ciutesting.com

Beat the Hacker



Professional Certificate in Cyber Threat Hunting

1. Understanding Networking

Networking is important for threat hunters because it provides visibility across all platforms and is the first point of contact for a response. Threat hunting is a proactive approach to identifying cyber threats in an organization's network

2. Setting up our Hacking Lab

3. Working with Kali Linux OS

4. Reconnaissance

- 4.1 Recon using Using Whois Tool
- 4.2 Whatweb Stealthy Scan
- 4.3 Aggressive WTD on IP range
- 4.4 OSINT Analysis
- 4.5 theHarvester and Hunter.io
- 4.6 Recon with Sherlock
- 4.7 DNS Analysis
  - DNSRecon
  - DNSEnum
  - DNSMap

5. Scanning

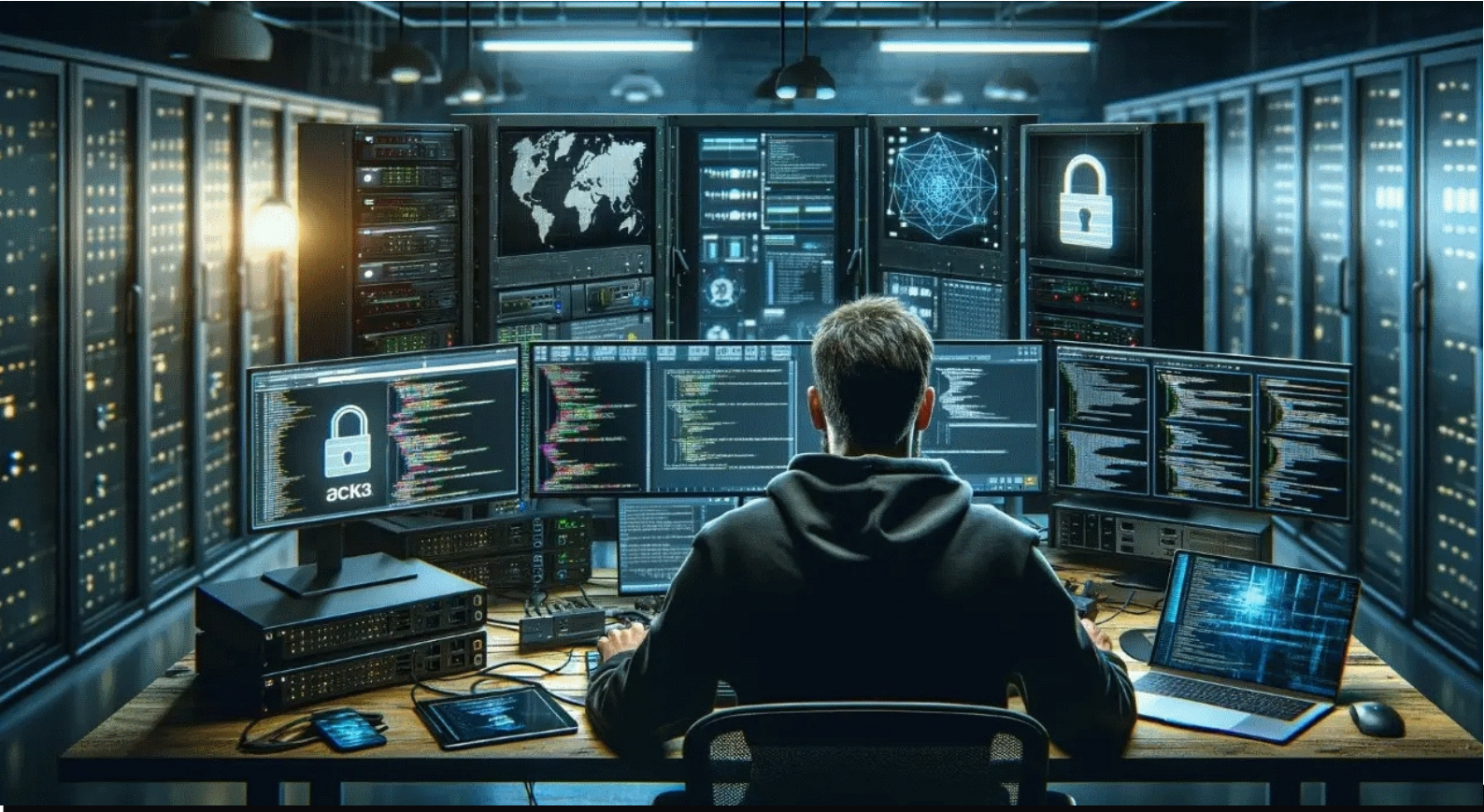
- 5.1 Theory Behind Scanning
- 5.2 Understanding TCP and UDP
- 5.3 Installing Vulnerable Virtual Machine
- 5.4 Netdiscover
- 5.5 Performing First Nmap Scan
- 5.6 Different Nmap Scan Types
- 5.7 Discovering Target Operating System
- 5.8 Detecting Version Of Service Running On An Open Port
- 5.9 Filtering Port Range _ Output Of Scan Results
- 5.10 What is a FirewallIDS
- 5.11 Using Decoys and Packet Fragmentation
- 5.12 Security Evasion Nmap Options

6. Vulnerability Analysis

- 6.1 Finding First Vulnerability With Nmap Scripts
- 6.2 Manual Vulnerability Analysis _ Searchsploit
- 6.3 Nessus Installation
- 6.4 Discovering Vulnerabilities With Nessus
- 6.5 Scanning Windows 7 Machine With Nessus
- 6.6 Wrap up

WhatsApp/Call: +91 8092431131

centre of PROFESSIONAL STUDIES
Technology Incubation Center CIU



Professional Certificate in Cyber Threat Hunting

7. Exploitation - Gaining Access

- 7.1 What is Exploitation
- 7.2 Reverse Shells, Bind Shells ..
- 7.3 Metasploit Framework Structure
- 7.4 Msfconsole Basic Commands
- 7.5 vsftp 2.3.4 Exploitation
- 7.6 Bindshell Exploitation
- 7.7 Telnet Exploit
- 7.8 Samba Exploitation
- 7.9 SSH Attack - Bruteforce Attack
- 7.10 Exploitation Challenge
- 7.11 Explaining Windows Setup
- 7.12 Eternal Blue Attack
- 7.13 DoublePulsar Attack
- 7.14 BlueKeep Vulnerability
- 7.15 Routersploit
- 7.16 Router Default Credentials

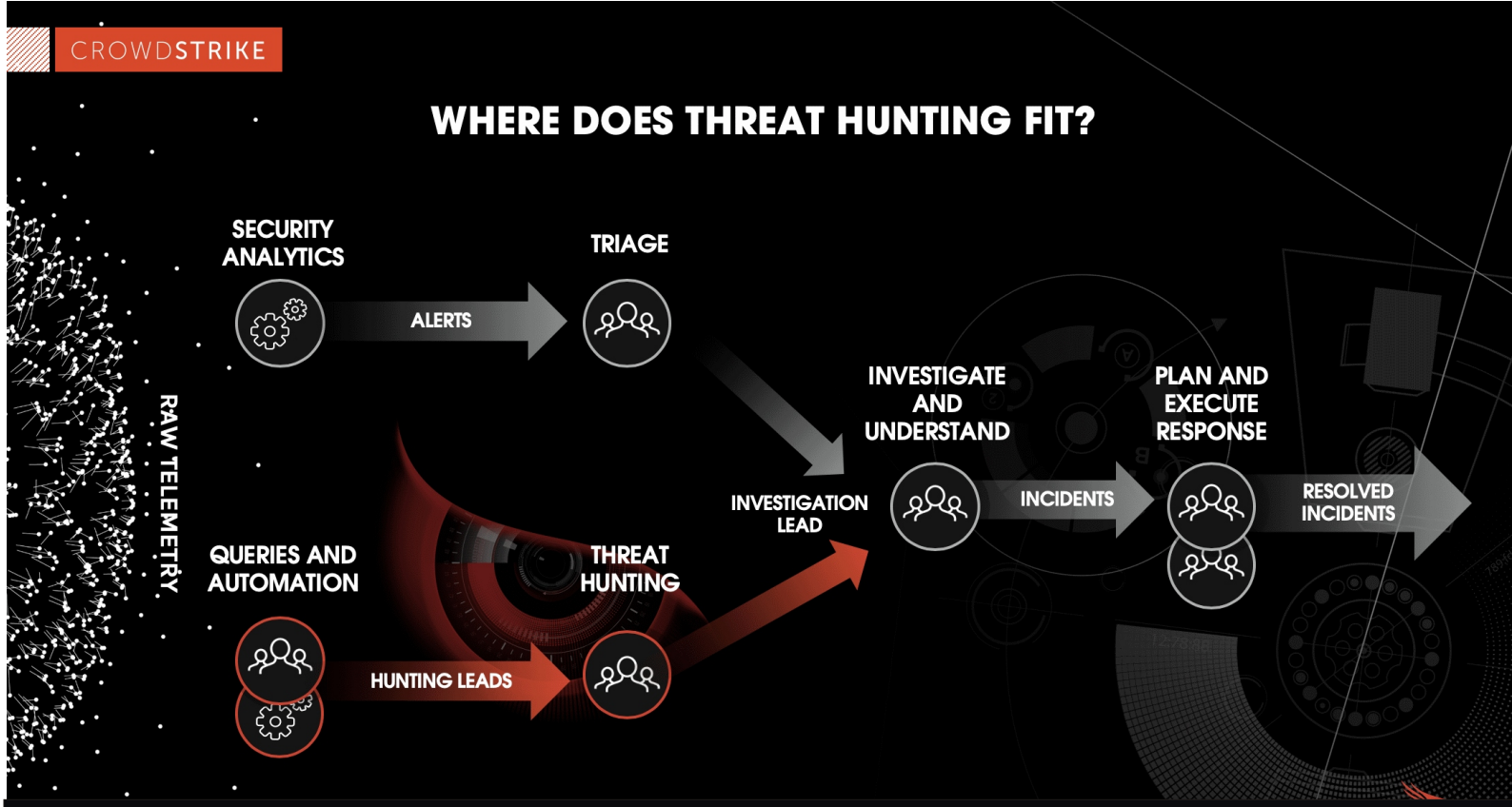
8. Gaining Access (Viruses, Trojans, Payloads ...)

- 8.1 Generating Basic Payload With Msfvenom
- 8.2 Advance Msfvenom Usage Part 1
- 8.3 Advance Msfvenom Usage Part 2
- 8.4 Generating Powershell Payload Using Veil
- 8.5 TheFatRat Payload Creation
- 8.6 Hexeditor Antiviruses
- 8.7 Making Our Payload Open An Image

9. Post Exploitation - Elevating Privileges, Extracting Data, Running Keyloggers

- 9.1 Post Exploitation Theory
- 9.2 Meterpreter Basic Commands Part 1
- 9.3 Meterpreter Basic Commands Part 2
- 9.4 Elevating Privileges With Different Modules
- 9.5 Creating Persistence On The Target System
- 9.6 Post Exploitation Modules
- 9.7 Exploitation Recap

WhatsApp/Call: +91 8092431131



Professional Certificate in Cyber Threat Hunting

THE CHALLENGE

Cobalt Strike gives you a post-exploitation agent and covert channels to emulate a quiet long-term embedded actor in your customer's network. Malleable C2 lets you change your network indicators to look like different malware each time.

This channel is open to bad guys as well as defenders like you. It is challenging for defenders to combat new sophisticated attacks evolving each day. Network hunting is the only way to protect against smart hackers.

Why EDR and XDR Will Always Fail Against Sophisticated Payloads

Six of the most formidable techniques that expose the limitations of Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) systems, revealing why these powerful defenses can fail in the face of sophisticated payloads from an Offensive Security perspective

Network Monitoring: Intrusion Detection Using Zeek

10. Why EDR and XDR Will Always Fail Against Sophisticated Payloads

Here are 6 of the sophisticated techniques that make EDR and XDR-based and similar solutions incapable to deal with

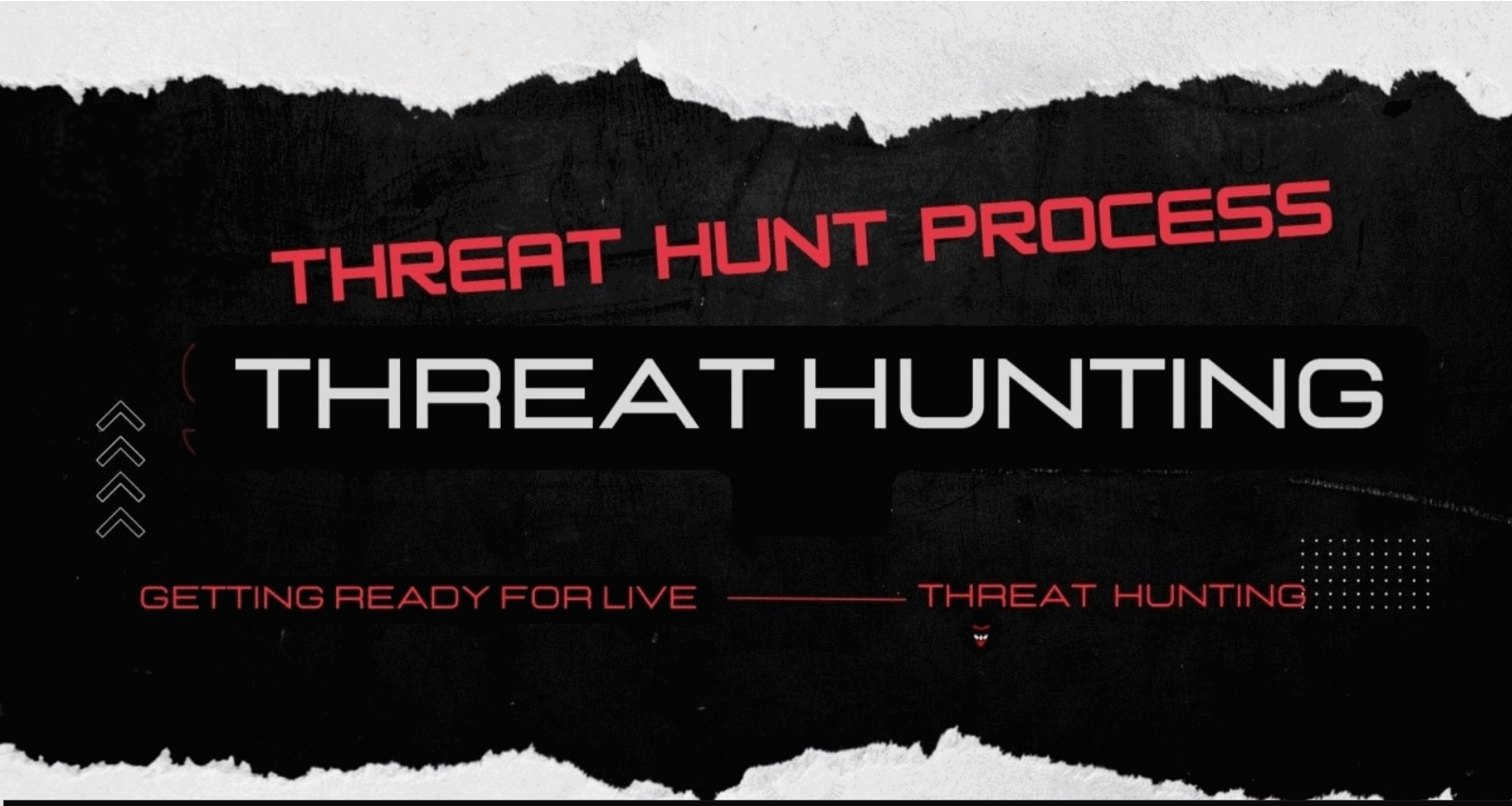
- 10.1 The Unpredictability of Unknown Signatures
- 10.2 Timed Payloads: The Perfect Bait
- 10.3 File Pumping and Backdooring: Double Trouble
- 10.4 Polymorphic Encoding
- 10.5 Memory Injection and Code Execution
- 10.6 Code Injection via Process Hollowing

Zeek Instrusion Detection as the first step of threat hunting when EDR/XDR/SIEM fail

- 10.7 Introduction to the Capabilities of Zeek
- 10.8 An Overview of Zeek Logs
- 10.9 Parsing, Reading and Organizing Zeek Log Files
- 10.10 Generating, Capturing and Analyzing Network Scanner Traffic
- 10.11 Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic
- 10.12 Introduction to Zeek Scripting
- 10.13 Introduction to Zeek Signatures
- 10.14 Advanced Zeek Scripting for Anomaly and Malicious Event Detection
- 10.15 Profiling and Performance Metrics of Zeek
- 10.16 Application of the Zeek IDS for Real-Time Network Protection

WhatsApp/Call: +91 8092431131

centre of PROFESSIONAL STUDIES
Technology Incubation Center CIU



Professional Certificate in Cyber Threat Hunting

THREAT HUNTING

We will spend most of this class analyzing PCAP files for Command and Control (C2) communications in order to identify malware back channels. It is assumed that the student will already understand the basics of network threat hunting, so we can immediately jump into applying that knowledge. The goal will be to create a threat hunting runbook that you can use within your own organization in order to identify systems that have been compromised

WORKING WITH RITA

Real Intelligence Threat Analytics (R-I-T-A) framework for detecting command and control communication through network traffic analysis. The RITA framework ingests Zeek logs in TSV or JSON format, or PCAPs converted to Zeek logs for analysis

11. Cyber Security Scripting for Threat Hunting

- 11.1 Network Traffic with Long Connections
- 11.2 Network Traffic with consistent busy traffic
- 11.3 Beacon Analysis
- 11.4 Scripting tool for Beacons
- 11.5 Scripting for http traffic for finding web anaomalies
- 11.6 Scripting for TLS and SSL traffic analysis
- 11.7 Scripting for IP, Proxy and SSL based beacons

12. Real Intelligence Threat Analytics (RITA)

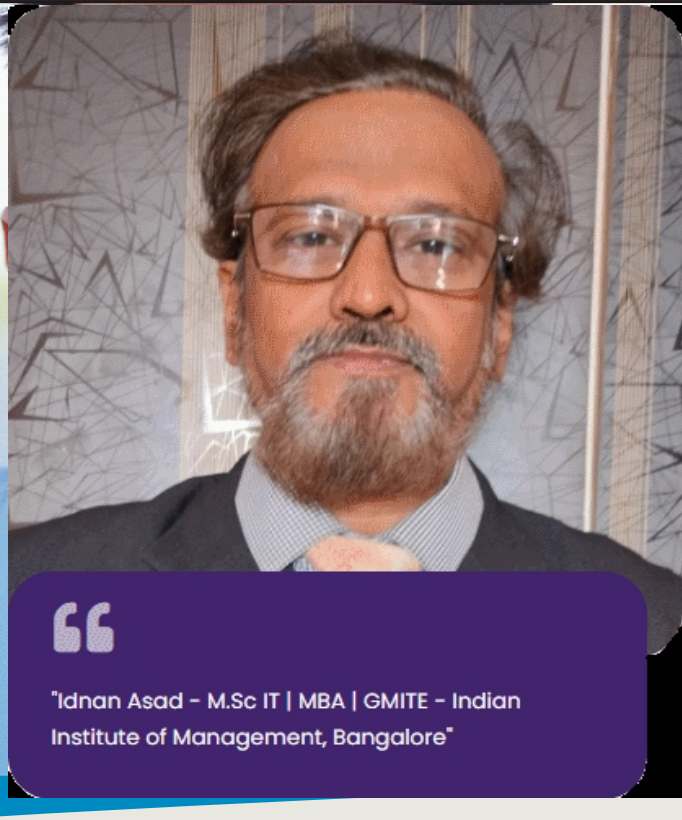
- 12.1 RITA Introduction
- 12.2 RITA integration with Zeek
- 12.3 Working with network datasets using RITA
- 12.4 RITA in Threat Detection with Zeek
- 12.5 RITA for beacon detection
- 12.6 RITA for exploded-dns
- 12.7 Threat Detections with User Agents
- 12.8 RITA with Fully Qualified Domain based Threats
- 12.9 RITA with long connections

WhatsApp/Call: +91 8092431131

Meet the Trainer
24 years experience in Network Security and Cyber Security Domain

CEO of Cambridge Intercontinental University ' USA

Author of several books and courses in IT Security and Enterprise Networking at university level for under-graduate and post-graduate courses.



Courses Accredited by QAHE ' USA

About the Trainer

A seasoned entrepreneur with a demonstrated history of working in Information Technology & IT Security Education. Author of several IT Security books, Skilled in Business Planning, Cyber Security, Database, IT Service Management, General Management, and Pre-sales. Strong professional with a GMITE focused in IT from the Indian Institute of Management, Bangalore.

Activities : Network Security Integration and Training, Telecommunication Education, Data Networks & Cybersecurity Workshops.

Linkedin : https://in.linkedin.com/in/idnan-asad

University: https://cambridgeuniv.org/courses/idnan.html

Technology Incubation Center CIU

C/o Maria International School
Jumman Colony, Baragain Road,
Ranchi -834009
WhatsApp/Call : +91 8092431131

Website : www.ciutesting.com

Technology Incubation Center CIU

List of certified candidates @ www.cambridgeuniv.org/alumni

Over 145000 Certified Candidates Globally

PARTIAL STUDENT'S LIST OF TIC CIU CERTIFICATIONS

Siddharth Yeshwanth	Hyderabad	General Electric
RAJIB BANERJEE	Kharagpur	IBM
Arindam Patra	Jamshedpur	IBM
Ashok Yadav	Jamshedpur	IBM
Subhajit Das	Kolkata	R S Software (I) Ltd
Rajtilak Majumder	Kalyani	Globsyn Technologies
John Mathew	Secunderabad	GENPACT IT Services
Vinay Prabhakar	Mandya	TATA TELESERVICES
Rabi Sankar	Kolkata	Dishnet Wireless Limited
Sivaram Krishna	Tirupati	CMC Limited,
Ratna Karbhowmik	Kolkata	AREVA T&D India Limited
Guru Moorthy	Bangalore	Microland
Mir Mohsin Hossain	Dhaka	City Bank
Anirban Dey	Kolkata	Hong Kong Bank
Rajneesh Chaturvedi	New Delhi	Aviva Life Insurance
Chidambaram M.	Bangalore	ACCEL ICIM Frontline Ltd
Sandeep Bhargava	Jaipur	Ericsson India Private Limited
Jyotirmoy Roy	Kolkata	CMS Computers Ltd
Md Jainul Hoque	kolkata	Videocon Industries Ltd.
Aymen Hussein	Riyadh	New Horizons
Muhannad Al-Sraihiny	Riyadh	New Horizons
NAGENDRA PRASATH	Chennai	BHARTI TELEVENTURES LTD
Md Ithesham Feroz	Hyderabad	GE Capital
Pankaj Vibhute	Mumbai	Tata Consultancy Services
Karthik Subramaniam	Coimbatore	HCL Technologies
Vivek Sen	Khargapur	IBM India Limited
SANJEEV SHARMA	HARYANA	NOKIA INDIA PRIVATE LIMITED
Chandra Banerjee	Kolkata	Ontrack Systems Ltd
Anirudha Joshi	Mumbai	Wipro Infotech Ltd
Anjani Dwivedi	Satna	Air tel
Faiz A. Roomi	Patna	IGNOU
Khaled Abdo	Salalah	Dhofar University
Vijayasekar	Coimbatore	Vidyasagar College of Arts & Sc
S. VenkateshHegde	Columbia	University South Carolina
Gaurav Bisht	Delhi	VSNL
Mohd Shahid	Delhi	VSNL
RAKESH PURKAIT	KOLKATA	VSNL
T. Sudhakar	Banglore	STPI
Moolaveesala V	Visakhapatnam	Software Technology Parks of India
EMMANUEL ASIMADI	Accra	Ghana Telecom
Muhammad Ibrahim	hosur	IIHT
Sherif Awad	Alexandria	Eltawil international trade
Anthony Elue	Enugu	Rainbownet ltd
Mohamed Mansour	Alexandria	Misr Chemical Industrials
Jitendra Shah	Jaipur	JEC
REA BELFON	PORT OF SPAIN	IN EXCESS LTD
Gaurav Chhabra	New Delhi	Theikos
Nirmalya Pal	Kolkata	Assuredhost
Chetan Thakur	Pune	Bluelane Tech Inc.
Snehal Baviskar	Ambernath	Ashtech Infotech Pvt.Ltd
Andrew Shoko	Harare	Powertel Communications
Edgardo Cosme-Vel	Ceiba	Aleut Communications
Stanley kumbol	Accra	Ghana telecom
Rajiv Kumar	Gandhinagar	GSWAN
Henry Arockiaraj	Coimbatore	RGM
Christy Elias	Bangalore	Webspectrum
Pratesh Pulayin	RAJKOT	ICENET.NET LTD
Michel Fahmy	Cairo	Telemetry MWRI
Mohammad Syed	Austin	T.W.C
Kaustuva Chatterjee	Kolkata	Bhart Telesoft