Course: Cyber security

Program: Basic Cyber security Bootcamp program

Duration: 1 week | Certified Training

Overview

In today's world, organizations must be prepared to defend against threats in cyberspace. Decision makers must be familiar with the basic principles and best practices of cybersecurity to protect their enterprises. Sessions will address information security, ethical and legal practices, and mitigating cyber vulnerabilities. Participants will also learn about the process of incident response and analysis. The content is targeted at ensuring the privacy, reliability, and integrity of information systems.

Cybersecurity is a very large subject, and therefore this course is only intended to cover the basics of the current leading and pressing cybersecurity topics. We cover the introduction of a topic and after the fundamentals, you can explore further on your own. The goal is for participants to understand the utility of each topic.

Participant Takeaways:

The participants of this course will be able to:

1. Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.

2. Determine computer technologies, digital evidence collection, and evidentiary reporting in forensic acquisition

3. Incorporate approaches to secure networks, firewalls, intrusion detection systems, and intrusion prevention systems.

4. Examine secure software construction practices.

5. Understand principles of web security

6. Incorporate approaches for incident analysis and response

7. Incorporate approaches for risk management and best practices

Introduction **3 Hrs**

1. What is a computer?

2. Operating System and its kinds

3.What is internet?

4. How Internet Works?

5.Types of Hackers

6. Current Scenario

7. Concept of Virtualization

8. Setting up a hacking playground for practice

Reconnaissance **4 Hrs**

1. Effective Use of Who.is Database

2. Using archive.org to gather information from old version of websites

3. Active and Passive Reconnaissance techniques

4. Using Maltego to make Personal investigations easier

5. Collecting Information from various search engines like Google, Shodan.io, Censys.io

6. Email Tracking.

7. Gathering information from meta content of images (Steganography)

8. Email Analysis to find out Spoofing

Scanning **7 Hrs**

1. What is IP Address?

2. What is MAC Address?

3. TCP / IP Protocols

4. Data packets analysis in a network using Wireshark

5. Banner Grabbing and OS Fingerprinting

6. Hands on training on Packet capturing techniques

7. Namp & IP Enumeration

8. Vulnerability Analysis

9. Using Publicly available exploits

Gaining Access **8 Hrs**

1. Hardware and software Keyloggers

2. Rubber Ducky and Badusb Attacks

3. HID Emulation to break Android PIN & Pattern (Teensy)

4. Building Windows Password Remover Tools

5. Using Live Boot Techniques to gain files access to locked apple laptops and PC

6. RAT and Trojans (PC and Mobile Platforms)

7. Botnets and C&C

8. Basics of Metasploit

9. Backdooring Techniques

10. Sniffing and Spoofing (MITMF)

11. Denial of Service and Distributed Denial of Service

12. Load Balancers and Honeypots

13. Effective use of publicly available exploits from exploit-db

Forensics **4 Hrs**

1. Digital Forensic Framework (DFF) (Windows and Linux)

2. Easeus Data Recovery

3. Android Data Recovery

4. USB History Forensics

5. Ghosting Hard Disk for later analysis

6. Andriller (Cracking PIN and other Forensics like Message, Contact, Account Data Gathering which includes Facebook, WhatsApp, viber etc..,)(Free Police License for 6 months)

Covering Tracks **3 Hrs**

1. Onion Routing and Tor Browser

2. Exploring Darknet and Deep web to know about advancements.

3. Proxy Server

4. Proxy Chaining

5. Evolution of Crypto Currencies

6. How VPN Works

7. Setting up VPN servers for remote access of tools

8. Clearing Tracks (Countermeasures to recover them)

Wireless Hacking **5 Hrs**

1. Leveraging wireless forensics to find the open networks

2. WIFI Cracking techniques

3. EVIL Twin attack

4. WIFI Jamming

5. Bluetooth Sniffing

6. GSM Sniffing using Special tools like Stingray

7. Build a gsm sniffing tool using Raspberry Pi , BladeRF and YateBTS

8. Cell Phone Signal Jamming and isolation.

Hardware Tools **6 Hrs**

Teensy

Rubber Ducky

PWN Pi

Alfa-card

BladeRF

Note: - Most of the training part will be practical with real case scenarios.