Faysal Aziz

Cyber Incident Response

FA-0473 · 2 days

Cybersecurity

Introduction

&

and Penetration Testing

An incident response plan is a documented, written plan with 6 distinct phases that helps IT professionals and staff recognize and deal with a cybersecurity incident like a data breach or cyber attack. Properly creating and managing an incident response plan involves regular updates and training. This course is designed to do just that. This course is focused on the practical side of penetration testing as well as the theory behind it.

Duration

2 days

Course Outcome

- Have a high level overview of the response process
- Understand the 6 phases of an incident response plan
- Effectively prioritize the response to a security incident
- Build a computer security incident response team (CSIRT)
- Develop an incident response action plan
- Post-incident activity
- Understand the GDPR
- Detect ARP poisoning and protect your self and your network against it.
- Use more than 20 penetration testing tools such as ettercap, wireshark, aircrack-ng suit ...etc.
- Combine individual attacks to launch even more powerful attacks.
- Perform Penetration Testing

- Perform Reverse Engineering for Forensics
- Take necessary measures to prevent cyber attacks
- Secure networks

Prerequisites

- Basic understanding of the current cybersecurity ecosystem
- Basic understanding of analysis of hacks on computers and networks
- Basic understanding of Risk Management
- Basic linux (preferably debian build such as kali)

Training outline

1. Threat modeling

2. Building a CSIRT

3. The Phases of IRP

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery

4. GDPR Standard

5. GDPR Incident Response Methodologies

6. Industry specific use case

7. Penetration Testing

1. SQL injections
2. Burp Suite
3. XSS

4. File upload Vulnerability
5. Command Line Execution
6. Havij

8. Reverse Engineering

1. Software Hacking
2. Virus illustration
3. Firewall Bypassing

9. Prevention & Security

1. Securing Your Network From The Above Attacks
2. How to Configure Wireless Security Settings To Secure Your Network
3. Detecting ARP Poisoning Attacks
4. Detecting Suspicious Activities using Wireshark

10. Assessment

NOTE: This course requires lab.

© 2026 Faysal Aziz · Kuala Lumpur