Hacking One è un idea :

Winitalia

Ethical Hackers
Guardians Group
Ad providendum virtutis studio et cognitione



Winitalia

Via Don Giovanni Bosco, 57

Civitanova M. (MC)

ORE 09:00

PER MAGGIORI INFORMAZIONI ED ISCRIZIONI : **http://www.ehg2.com/H1**

Perché..

..le informazioni di ognuno di noi, i database gestiti e custoditi dai sistemi informativi di aziende pubbliche e private rappresentano una "risorsa strategica" di altissimo valore che deve essere tutelata e protetta per garantire la privacy e l'IT Governance di un intero paese. ***Sicurezza, Riservatezza, Integrità dei Dati, Privacy*** *e* ***Controllo delle Informazioni****, sono oggi i nuovi driver che ogni giorno, spesso in maniera intangibile, interagiscono e* ***modificano l'esistenza*** *di paesi, singoli cittadini…****di tutti noi****. Proprio per questo sono oggetto di forte interesse da parte di criminali e malintenzionati.*

Come..

..Hacking One è un ***training formativo avanzato sulla sicurezza informatica, un laboratorio dal vivo che mostrerà e svelerà le più moderne metodologie di attacco****: dai singoli computer collegati ad internet alla infrastrutture ICT complesse.* ***Dimostrazioni pratiche*** *dove saranno spiegate le tecniche di intrusione e di attaco a sistemi informativi di tipo diverso e i sistemi di protezione e controllo dei dati memorizzati.* ***Manipolazione delle informazioni, violazioni della sicurezza*** *e* ***attività di contrasto*** *saranno rappresentate in uno scenario di connessione globale dove ogni utente, sia singolo privato, azienda, che ente governativo, può essere vittima di criminali informatici e cyber terroristi. Gli Ethical Hacker del gruppo di ricerca EHG2* ***rappresenteranno*** *le varie tematiche collegandole tra loro attraverso un innovativo e avvincente filo narrativo basato sulla ricostruzione di* ***vicende realmente accadute.***

Chi..

..EHG2 (Ethical Hackers Guardian Group) è un gruppo di ricerca formato da esperti altamente specializzati che si occupa da anni di sicurezza informatica e nuove tecnologie ICT. La mission di EHG2 è lo studio di metodologie innovative per la formazione e l' informazione sui temi della sicurezza ICT e sul corretto utilizzo delle nuove tecnologie (sia per il normale utilizzatore che per i professionisti del settore).

Target : Il seminario è rivolto a tutti i responsabili e tecnici informatici, esperti e consulenti della sicurezza ICT. Al termine del seminario sarà rilasciato l'attestato di partecipazione.

Adesioni : La quota di partecipazione al seminario è di €199,00 (iva compresa), i posti sono limitati. Si prega di verificare la disponibilità e confermare l'adesione al seguente indirizzo:

http://www.ehg2.com/h1

A tutti gli iscritti verrà fornito il materiale del training in formato elettronico.

Per maggiori informazioni : info@ehg2.com

Programma

Ore 09:00 – **Registrazione e Welcome Coffee**

Ore 09:20 – **Inizio Lavori** – introduzione

Ore 09:30 – **HackingOne Sessione 1 – Anatomia di un Hacking : analisi e ricostruzione di un attacco**
(in questa sessione verrano mostrate le principali metodologie e tecniche di attacchi informatici sulla base narrativa di eventi realmente accaduti)
principali argomenti trattati :

- come si effettua l'information gathering di una rete/host vittima
- preparazione dell attacco informatico (reliability check, planning)
- Dimostrazione dell'attacco pianificato :
  - come si realizza un attacco basato su shellcode per creare backdoor
  - come si realizza un worm per il keylogging ed elusione degli antivirus
  - come si realizza un attacco man in the middle
  - come si realizza un attacco mirato alla cattura di credenziali (ftp,telnet,https,etc.)
  - come si realizza un attacco di phishing attraverso l'omografia.
  - cracking delle password su sistemi operativi Windows, Linux e MAC
  - Penetrazione di sistemi operativi attraverso l'utilizzo di exploit
  - come si realizza un attacco di cracking di reti Wireless WEP e WPA
  - come si realizza un attacco ai device Bluetooth di telefoni cellulari
  - come si realizza lo Sniffing ed intercettazione di chiamate VOIP

Ore 13:00 – Break – Branch

Ore 13:30 – **HackingOne Sessione 2 – "best practices" di computer forensic ed indagine digitale**

- Data Carving: come effettuare il recupero e la ricostruzione di dati cancellati e/o occultati
- Gestione delle prove digitali: le implementazioni legali
- Metodi di crittoanalisi di informazioni cifrate
- Dimostrazione dei principali metodi di steganografia delle informazioni e dei file system
- Manipolazione delle informazioni e social engineering: dimostrazioni

Ore 15:00 – **HackingOne Sessione 3 – Hardening dei sistemi ICT : principali linee guida**

- linee guida all' implementazione di reti sicure (Wired e Wireless: architetture e servizi)
- Hardening dei principali servizi di Host Microsoft, Linux e Mac
- Linee guida per la realizzazione del regolamento degli utenti
- procedure di gestione degli incidenti informatici
- I principali aspetti legali e burocratici da verificare

Ore 16:30 – Tavola rotonda

Ore 17:00 – Fine lavori