CURS SEMIPRESENCIAL

Ciberseguretat, Hacking ètic, pentesting i Seguretat de Computadors

23, 25, 29 i 30 de març, 5 i 7 d'abril de 2022

Presentació

En tots els àmbits professionals es necessiten persones expertes en seguretat informàtica perquè gestionin i prenguin decisions de planificació de la seguretat informàtica de l'entitat.

No és necessari ser membre de la direcció IT, atès que hi ha posicions que permeten tenir una influència directa sobre quines decisions s'han de prendre en cada moment.

No és cap sorpresa que la ciberseguretat encapçali les preferències de les entitats en els seus processos de transformació digital. La Internet de les Coses, el Big Data o el Cloud Computing són tendències que requereixen d'una bona ciberseguretat per resultar efectives.

Disposar d'unes comunicacions fiables i segures és fonamental en qualsevol sistema equipat amb tecnologia d'Internet. Per aconseguir-ho, la ciberseguretat aplica a aquests actius diverses capes de protecció en diferents nivells per assegurar-ne la protecció. No en va, el 40% dels ciberatacs causen la interrupció de les operacions i els processos, mentre que un 39% provoquen la pèrdua d'informació confidencial.

FEDERACIÓ DE MUNICIPIS DE CATALUNYA

programa

1. **Footprinting and Reconnaissance**
2. **Scanning Systems and Enumeration**
3. **Vulnerability Analysis**
4. **System Hacking** – Introducció a Windows
5. **System Hacking** – Windows Privilege Escalation
6. **System Hacking** – Introducció a Linux
7. **System Hacking – Linux Privilege Escalation**
8. **WiFi Security**
9. **Sniffing, Detection and Prevention**
10. **Hacking Web Servers** – I
11. **Hacking Web Servers** – II

LABORATORIS

Durant el curs es desenvoluparan 6 laboratoris (en grups de tres persones) on es configuraran els següents escenaris de hacking:

Footprinting, Reconnaissance, Scanning Systems and Enumeration

- Identificació de xarxes (p. ex. a ripe-net)
- Cerca de e-mails corporatius i patrons
- Atacs a zones DNS mitjançant fierce i recon-ng.
- Cercar equips i mails mitjançant Google hacking Database, TheHarvester i Maltego
- Identificació de xarxes i dominis amb dnsdumpster

Network Security and System Vulnerabilities (GMargarit)

- Escaneig de xarxes avançat amb nmap
- Descobriment dels ports oberts i serveis de xarxa
- Descobriments de noms d'usuari al Directori Actiu o serveis equivalents
- Utilització de Nessus.

Windows System Hacking

- Exploit windows unpatched vulnerability (kernel, software, etc.)
- Lateral movement
- System Account privilege escalation
- Getting Information
- SAM dump and NTLM hack

Linux System Hacking

- Exploit windows unpatched vulnerability (kernel, software, etc.)
- Lateral movement
- Abusing SUID permissions
- Leveraging from cron tasks
- Sudo permissions

Web Server Hacking

- Automatic scans: Nikto, wpscan...
- Parameter tampering attacks
- Cross-Site-Scripting and CSRF
- Command Injection and File Inclusion Attack
- Reverse Shell

Sniffing, Detection and Prevention

- Detecting traffic with Wireshark
- Blocking connections with Snort
- Configuring Windows Firewall (u otra opción)

Metodologia

- Curs semipresencial que combina classes presencials amb sessions a distància.
- Laboratoris pràctics (simulant un entorn real).
- Estudi autònom en l'aula virtual.
- Teoria i pràctica es combinen mitjançant mètodes interactius per facilitar l'aprenentatge i aprofitar l'experiència i el coneixement del grup.

Docent

Genís Margarit i Contel. Enginyer en: Enginyeria de Telecomunicacions i Enginyeria de Sistemes Electrònics per la Universitat Politècnica de Catalunya - UPC. Auditor de ciberseguretat els darrers 15 anys. Va fundar la seva empresa de consultoria en ciberseguretat fa deu anys. Compagina la seva tasca amb la docència a la Universitat Pompeu Fabra (UPF) i com a instructor d'EC-Council. És membre de l'Associació Professional Espanyola de la Privacitat, fundador del grup de seguretat de Telecos.cat, expert tècnic del European Privacy Seal i Privacy by Design Ambassador.

Durada

24 hores

Horari

De 9.30 a 14.00 hores

Destinataris

Responsables de seguretat de la informació i àrea de tecnologies de la informació i la comunicació. **El seguiment del curs requereix un bon nivell d'expertesa en xarxes informàtiques i en administració de sistemes operatius.**

Lloc de realització del curs

Sessions presencials: **25 i 30 de març i 7 d'abril**
UPF-BSM (Barcelona School of Management) Universitat Pompeu Fabra, carrere Balmes, 134. Barcelona

Sessions virtuals: **23 i 29 de març i 5 d'abril.** Plataforma Zoom

Certificat

Es lliurarà un certificat d'aprofitament a les persones que acreditin l'assistència a un 80% de les hores lectives del curs i que responguin correctament un test d'avaluació de l'assoliment dels coneixements bàsics del curs o realitzin amb èxit les activitats requerides pel docent en el decurs de l'acció formativa. El test es respondrà electrònicament a través d'un enllaç que els alumnes rebran per correu electrònic i que hauran de lliurar dins del termini establert.

Inscripcions

El termini d'inscripció finalitza el dia **15 de març de 2022**. La inscripció és gratuïta i el nombre de places és limitat. Per a la selecció de les inscripcions es tindrà en compte la cobertura territorial (s'afavorirà la participació del màxim nombre d'ajuntaments possible) i l'ordre de recepció de les sol·licituds. La formalització de la inscripció es farà per mitjà del formulari que trobareu al web de la Federació: www.fmc.cat.

Organitza:
Federació de Municipis de Catalunya

FEDERACIÓ DE MUNICIPIS DE CATALUNYA