

Introducció a la Seguretat Informàtica

Breu descripció del curs

Aquest curs és una introducció a la seguretat informàtica, concretament a l'auditoria d'aplicacions Web. Durant el curs es tractaran els principals tipus d'atacs a nivell Web així com formes d'evitar-los i corregir-los.

Coneixements previs

Es recomana que l'alumne conegui la sintaxi bàsica de SQL, tot i que es farà una introducció al curs. Els següents són requisits necessaris que s'assumirà que l'alumne coneix:

- Nocions bàsiques sobre el funcionament d'Internet
- Nocions bàsiques sobre HTML, JavaScript i PHP.
- Conèixer algun llenguatge de programació.

Temari

- **Tema 1:** Data Gathering.
Hores dedicades: 4h.
Punts tractats: Obtenció d'informació i rastreig, escaneig de ports.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç d'obtenir tota la informació disponible d'un cert objectiu fent servir les eines habituals per a l'obtenció d'informació.
- **Tema 2:** Bugs i Exploits.
Hores dedicades: 2h.
Punts tractats: Concepte de bug i exploit. Metasploit.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç de testejar les aplicacions en busca de bugs coneguts i d'exploitar-los en cas de trobar-los.

- **Tema 3:** Ocultació del rastre.
Hores dedicades: 1h.
Punts tractats: Proxies i xarxes d'anonimitat. Tor. Logs i zappers.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç d'utilitzar eines per ocultar la seva identitat, així com conèixer les eines que té l'administrador d'un sistema Linux per detectar les accions d'un atacant.
- **Tema 4:** Google Hacking.
Hores dedicades: 1h.
Punts tractats: Obtenció d'informació sensible amb Google.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç d'utilitzar Google per obtenir informació sensible de pàgines Web.
- **Tema 5:** Password Cracking.
Hores dedicades: 2h.
Punts tractats: Cracking remot i local. Hydra, Brutus. John the Ripper, Cain&Abel.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç de crackejar diferents tipus de xifrats i hashes utilitzant programes específics de cracking.
- **Tema 6:** HTTP, cookies i fuzzing.
Hores dedicades: 4h.
Punts tractats: Funcionament del protocol HTTP. Importància i perill de les cookies. Fuzzers.
Coneixements assolits: En acabar aquest tema, l'alumne coneixerà el protocol HTTP i serà capaç d'exploitar i preveure el principals bugs deguts a les cookies i els fuzzers.
- **Tema 7:** Principals bugs i atacs a aplicacions Web.
Hores dedicades: 6h.
Punts tractats: Path Traversal. Remote File Inclusion. Cross Site Scripting. Cross Site Request Forgery. SQL Injection. Blind SQL Injection.
Coneixements assolits: En acabar aquest tema, l'alumne serà capaç d'auditar pàgines i sistemes Web en busca de bugs i errors de seguretat, així com evitar-los i corregir-los.