Ethical Hacking – Documento per Vulnerability Assessment.

Visto il costante aumento delle vulnerabilità di sistema documentate ogni anno, si rende necessario ripetere l'attività di Ethical Hacking per impedire la perdita di informazioni preziose e salvaguardare la produttività aziendale.

Si richiede una offerta per la scansione di apparecchiature hardware sia verso il perimetro della nostra infrastruttura che verso alcune aree della rete interna.
L'offerta dovrà prevedere l'assessment di almeno 30 indirizzi interni e 7 esterni.

L'attività di Vulnerability Assessment dovrà essere espletata verso macchine con i seguenti sistemi operativi:

- Microsoft
- Unix / Linux
- Sun

Gli ambienti che dovranno essere testati saranno, di una o più, delle seguenti tipologie :

- Apparati di rete (router, switch, …)
- WEB server
- Application server
- FTP server
- Mail server
- DB server
- DNS

Le attività svolte al Vulnerability Assessment dovranno avvalersi sia di tool automatici che "attacchi" manuali.
Per ogni server dovranno essere riportate tutte le attività svolte.

Alla fine dell'attività di vulnerability assessment dovranno essere presentati i seguenti documenti:

- Documento Tecnico
- Presentazione Manageriale (esposta dalla società che effettuerà il vulnerability assessment)
- Presentazione tecnica

Nella presentazione manageriale si richiede un confronto tra i risultati emersi nel vulnerability assessment in Mediolanum ed altre società del settore finanziario e bancario.
Per le eventuali vulnerabilità riscontrate dovranno essere specificati i passi da seguire per ovviare i problemi trovati.

In allegato ci sono alcuni esempi di documenti riassuntivi relativi all'attività svolta, suddivisi tra Assessment interno ed esterno.


C:\Documents and Settings\luca\Desktop


C:\Documents and Settings\luca\Desktop