PAUTA DE EVALUACIÓN
SEGURIDAD Y AUDITORIA INFORMÁTICA
Docente: Alan Cartes Fica.
Evaluación Nº 1

Objetivo: Realizar un informe de reconocimiento pasivo a una empresa chilena o extranjera considerando los siguientes aspectos:

*-Dominios
*-Subdominios
*-Datos de contactos de registros
*-Cargos del Personal involucrado
*-Cuentas de email corporativas y personales
*-Publicaciones
*-Proveedores
*-Clientes
*-Documentos públicos
*-Metadatos
*-Sistemas OnLine

Se debe utilizar el sistemas operativo Kali Linux, bajo los siguientes comandos de reconocimiento pasivo:

Comandos Reconocimiento Pasivo

whois 1.1.1.1 (ip publica)
dnsrecon -d dominio.com
theharvester -d dominio.com -c -b all
goofile -d dominio.com -f pdf
metagoofil -d dominio.com -t doc –l (ele) 100 -n 20 -o /tmp/ -f /tmp/meta.html

pdfinfo -meta documento.pdf
exiftool all= archivo.pdf (con -all= archivo.pdf limpio los metadatos)

Tópicos del Informe:

1. Portada Institucional (3 pts.)
2. Introducción (10 pts.)
3. Reconocimiento Pasivo:
    a. *-Dominios (10 pts.)
    b. *-Subdominios (10 pts.)
    c. *-Datos de contactos de registros (15 pts.)
    d. *-Cargos del Personal involucrado (15 pts.)
    e. *-Cuentas de email corporativas y personales (10 pts.)
    f. *-Publicaciones (10 pts.)
    g. *-Proveedores (15 pts.)
    h. *-Clientes (15 pts.)
    i. *-Documentos públicos (10 pts.)
    j. *-Metadatos (10 pts.)
    k. *-Sistemas OnLine (10 pts.)
4. Bibliografía (5 pts.)
5. Conclusión (10 pts.)

Sitios de interés:

www.linkedin.com
www.archive.org
www.shodan.io
www.dateas.com/es
nmap.org/nsedoc
www.digitalocean.com
www.rapid7.com

Metodologías, estándares y políticas:

Metodologías:
OSSTMM - http://www.isecom.org/research/osstmm.html
ISSAF - http://sourceforge.net/projects/isstf/

Estándares:
- ISO/IEC 27002 - http://www.iso.org/iso/catalogue_detail?csnumber=54533
- PCI-DSS - https://es.pcisecuritystandards.org/minisite/en/
- HIPAA - https://www.hipaa.com/
- OWASP Top Ten. - https://www.owasp.org/index.php/Main_Page

Políticas:
- CIS - https://www.cisecurity.org/
- DISA STIG - http://iase.disa.mil/stigs/Pages/index.aspx
- FDCC - https://en.wikipedia.org/wiki/Federal_Desktop_Core_Configuration
- USGCB - http://usgcb.nist.gov/

Notas, Confidencialidad y Bibliografica

Bibliografia:

Ingenieria Social:
https://play.google.com/store/books/details?id=9gnUAgAAQBAJ

APT:
https://play.google.com/store/books/details?id=8aUfBQAAQBAJ

Kevin Mitnik:
https://books.google.cl/books?id=tGAxGQAACAAJ&sitesec=buy&hl=es&source=gbs_atb
https://books.google.cl/books/about/The_Art_of_Deception.html?id=OIy4F-8b_uEC&source=kp_cover&redir_esc=y

Metasploit:
http://www.amazon.es/Metasploit-The-Penetration-Testers-Guide/dp/159327288X

Certificaciones:
https://www.isc2.org/official-isc2-textbooks.aspx
http://www.amazon.com/Certified-Ethical-Hacker-All-One/dp/0071772294

Nexpose + Metasploit:
http://www.amazon.com/Mastering-Nexpose-Metasploit-Lab-Based-Approach/dp/0128010444

Puntaje total Tópicos: 158 pts.
Puntaje aprobatorio (nota 4): 95 puntos.

Ante cualquier ambigüedad favor remitir su consulta al email
alan.cartes@inacapmail.cl