

Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Analista de Seguridad Informática



Organiza



Enseñanzas Propias



Dpto. Lenguajes y Computación

Julio Gómez López

Capítulo 2. Buscar un vector de ataque

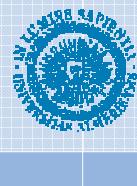
Contenido

Introducción

Localizar el
objetivo

Analizar el
objetivo

Introducción



Analista de Seguridad Informática

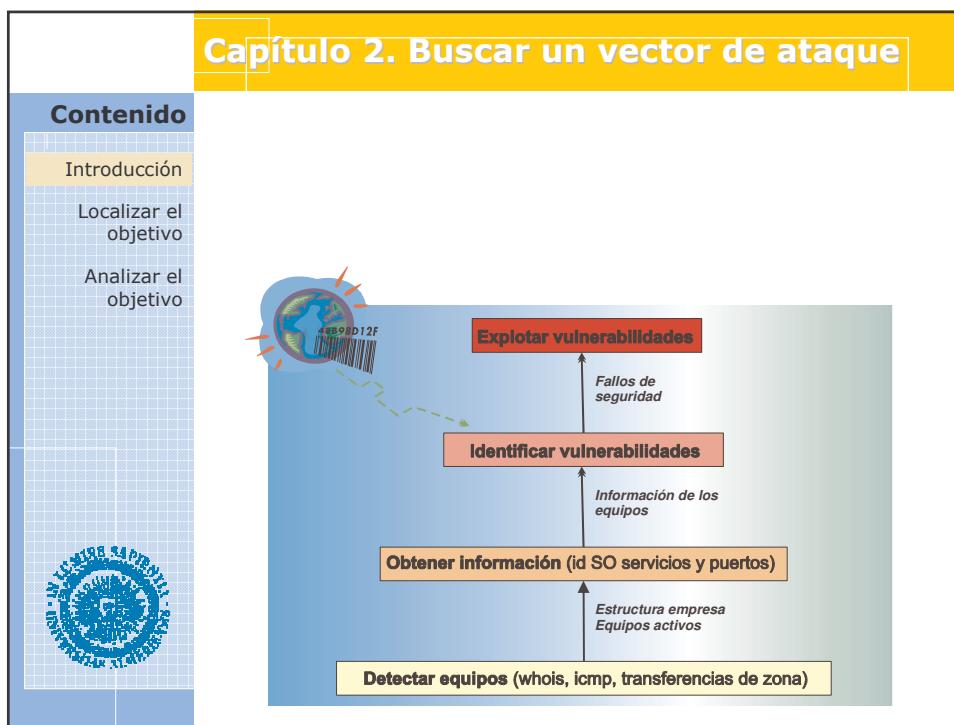
Capítulo 2. Buscar un vector de ataque

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Las reglas del juego</h4> <p>Entre la empresa y el analista hay que formalizar dos contratos:</p> <ul style="list-style-type: none">• Carta blanca. Contrato que firma la empresa y que le da libertad al hacker de hacer lo que quiera.• Confidencialidad. El analista firma un contrato en que se establece el carácter confidencial de los datos que encuentre <pre>graph LR; Analyst[Analista] -- "confidencialidad" --> Company[Empresa]; Company -- "carta blanca" --> Analyst;</pre>
---	--

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Las reglas del juego</h4> <p>Tipos de auditoría:</p> <ul style="list-style-type: none">• ¿Es una evaluación del sitio web?• ¿De la red externa? ¿de la interna?• ¿Es una evaluación física?• ¿Se puede utilizar ingeniería social?
---	--

Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

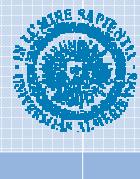
Capítulo 2. Buscar un vector de ataque

Contenido

Introducción

Localizar el objetivo

Analizar el objetivo



Localizar el objetivo

Capítulo 2. Buscar un vector de ataque

Contenido

Introducción

Localizar el objetivo

Analizar el objetivo



Bases de datos Whois
Consultas DNS inversas
Transferencias de zona no autorizadas
Barridos de pings
Trazado de rutas



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo

Capítulo 2. Buscar un vector de ataque

Base de datos WhoIS – sobre un dominio

DATOS DEL DOMINIO ALMERIMATIC.ES

Registrante: Almerimatic Sistemas Informáticos S.A.
Contacto Técnico: ARLS-ESNIC
Alfredo Ruiz
Maestro Padilla, 2, bajo
04008
Almería
ES
+34 950322211
alruiz@2000.es
Contacto Técnico: IMRS-ESNIC
Contacto Administrativo: FELL-ESNIC
Fecha Creación: 30/10/1997
Fecha Expiración: 30/10/2007
Servidores A2000.es
dns.a2000.es
dns.a2000.es

Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo

Capítulo 2. Buscar un vector de ataque

Base de datos WhoIS – sobre una dirección IP

<http://cqcountr.com/whois/>

IP Address : 194.187.219.89 [tor-proxy.vuokra.pirakka.com]
ISP : Tenue Oy
Organization : Tenue Oy
Location : Espoo, FI, Finland
City : Espoo
Latitude : 60°21'47" North
Longitude : 24°06'47" East

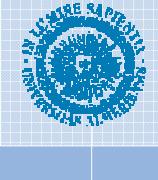


Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo



Capítulo 2. Buscar un vector de ataque

Consultas DNS inversas

Las consultas directas son necesarias para el correcto funcionamiento de internet ya que sin ellas no sería posible poner en el navegador una dirección web y obtener la página. Pero las consultas inversas no son necesarias pero si son muy peligrosas ya que si un atacante conoce todos los dominios que tiene su servidor es lógico que intente entrar por el dominio más vulnerable.

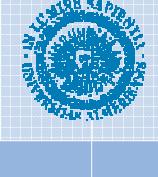
www.ual.es

directa → 150.214.156.62

← inversa

Contenido

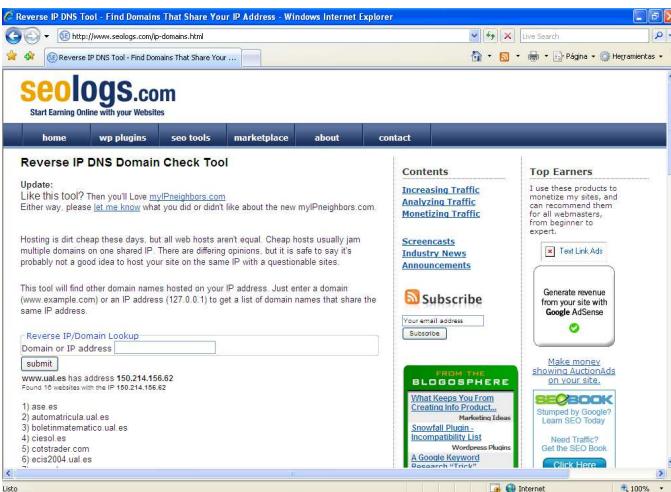
- Introducción
- Localizar el objetivo
- Analizar el objetivo



Capítulo 2. Buscar un vector de ataque

Consultas DNS inversas

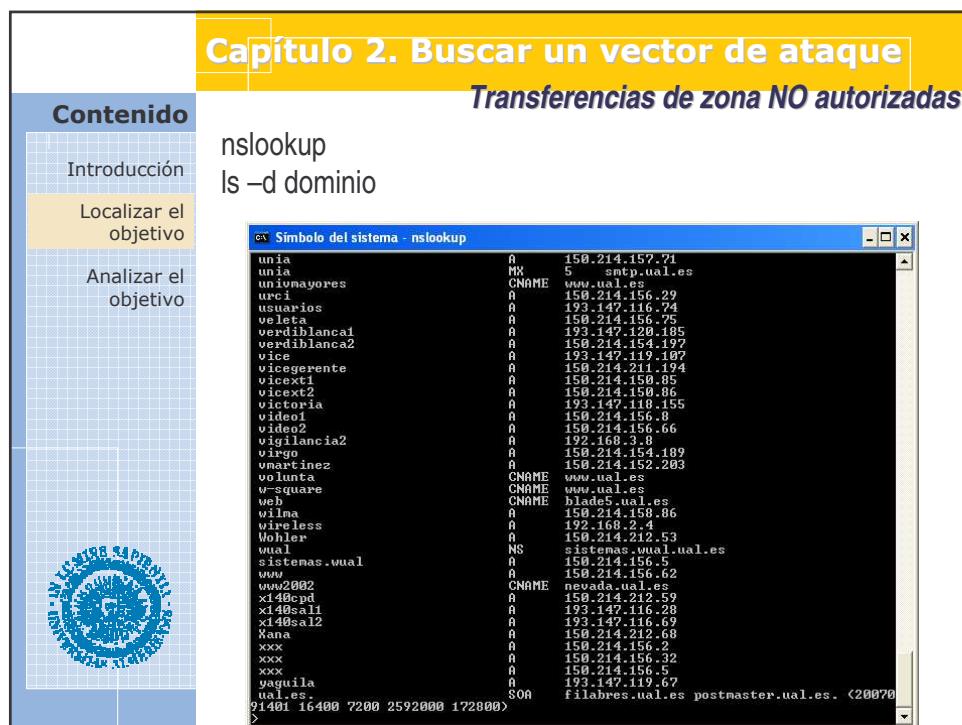
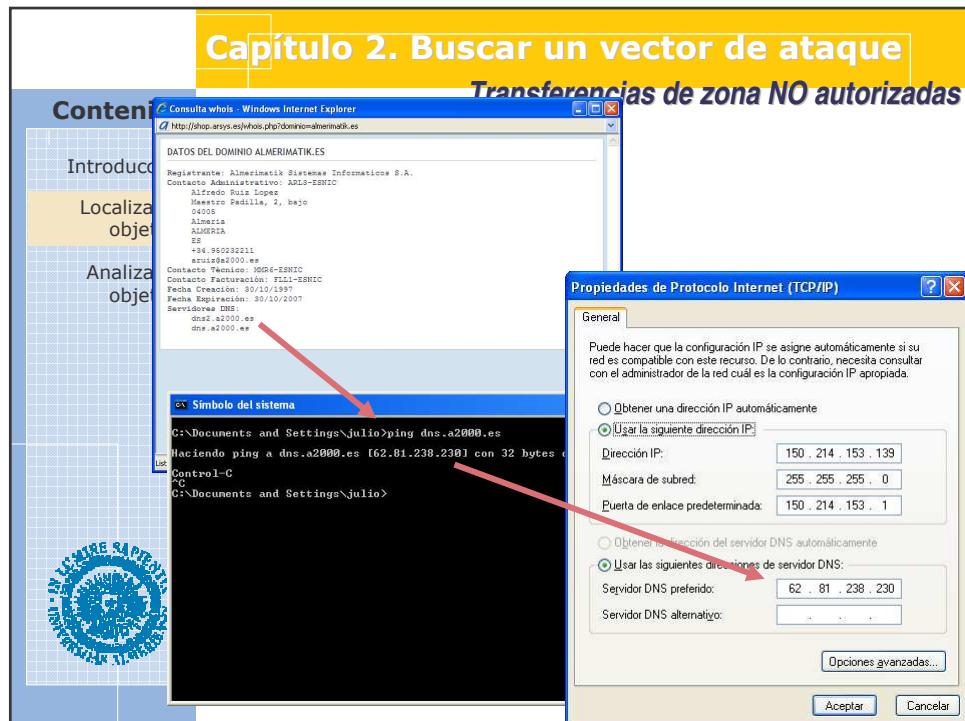
www.seologs.com/ip-domains.html





Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Capítulo 2. Buscar un vector de ataque

Barrido de pings

Contenido

- Introducción
- Localizar el objetivo
- Anализar el objetivo

El barrido de pings permite determinar los equipos activos de una red.

nmap -sP <dir de red>

Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo



Capítulo 2. Buscar un vector de ataque

RETO

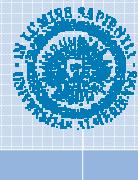
El reto consiste en obtener toda la información posible sobre la red en la que te encuentras. Para ello deberás realizar las siguientes tareas:

- Consulta los datos de registro del dominio
- Consulta inversa sobre el servidor www.ual.es
- Transferencia de zona del dominio en el que te encuentras
- Determina todos los equipos activos que hay en la subred donde te encuentras



Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo



Capítulo 2. Buscar un vector de ataque

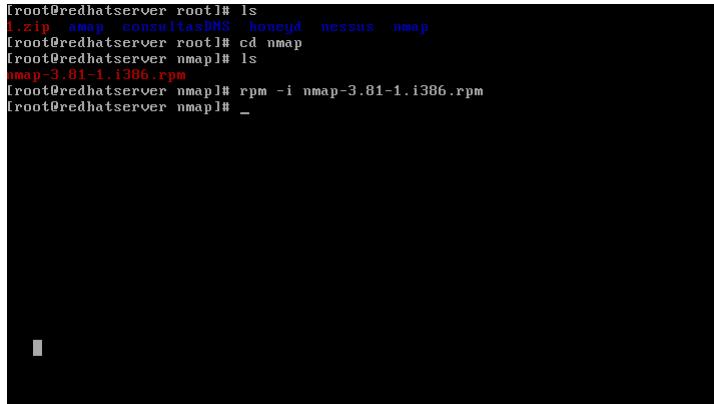
Analizar el objetivo



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

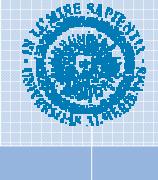
<p>Contenido</p> <p>Introducción Localizar el objetivo Analizar el objetivo</p> 	<h3>Capítulo 2. Buscar un vector de ataque</h3> <p>Los objetivos que se persiguen con la exploración de puertos son los siguientes:</p> <ul style="list-style-type: none">• Identificar los servicios que se están ejecutando en el sistema.• Identificar el tipo de sistema operativo instalado en el sistema.• Identificar las versiones o aplicaciones específicas de un determinado servicio.• Identificar las vulnerabilidades del sistema
---	--

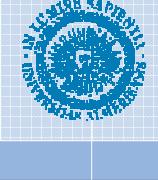
<p>Contenido</p> <p>Introducción Localizar el objetivo Analizar el objetivo</p> 	<h3>Capítulo 2. Buscar un vector de ataque</h3> <p><i>Identificar los servicios nmap</i></p> <pre>rpm -i nmap-3.81-1.i386.rpm</pre> 
--	--



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Identificar los servicios</h4> <p>nmap</p> <pre>nmap -sP <DIR RED> ejem. nmap -sP 172.16.0.0/16</pre>  <pre>[root@redhatserver root]# nmap -sP 192.168.0.0/24 Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2005-05-03 23:41 CEST Host 192.168.0.1 appears to be up. MAC Address: 00:40:F4:98:E0:62 (Cameo Communications) Host 192.168.0.46 appears to be up. Host 192.168.0.90 appears to be up. MAC Address: 00:0C:29:84:A1:5F (VMware) Nmap finished: 256 IP addresses (3 hosts up) scanned in 6.435 seconds [root@redhatserver root]# _</pre>
---	---

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Identificar los servicios</h4> <p>nmap</p> <pre>nmap <ip></pre>  <pre>Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2005-05-01 22:12 CEST Interesting ports on 192.168.0.1: (The 1646 ports scanned but not shown below are in state: closed) PORT STATE SERVICE 21/tcp open ftp 53/tcp open domain 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 1025/tcp open NFS-or-IIS 1080/tcp open socks 3001/tcp open nessusd 3005/tcp open deslogin 3006/tcp open deslogind 3372/tcp open msdtc 3389/tcp open ms-term-serv 4500/tcp open sae-urn 4557/tcp open fax 4559/tcp open hylafax 8080/tcp open http-proxy MAC Address: 00:40:F4:98:E0:62 (Cameo Communications) Nmap finished: 1 IP address (1 host up) scanned in 0.619 seconds [root@redhatserver nmap]# _</pre>
---	--



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Identificar el sistema operativo</h4> <p>nmap</p> <pre>nmap -O <ip></pre> <pre>[root@redhatserver root]# nmap -U 192.168.0.1 Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2005-05-02 10:52 CEST Interesting ports on 192.168.0.1: (The 1662 ports scanned but not shown below are in state: closed) PORT STATE SERVICE 38/tcp open http MAC Address: 00:0F:21:D7:CE:F9 (Scientific Atlanta) Device type: firewall/switch/WAP Running: SonicWall SonicOS, Enterasys embedded, Cisco embedded OS details: SonicWall SOHO firewall, Enterasys Matrix E1, or Accelerated Networks VoDSL, or Cisco 350 Access Point Nmap finished: 1 IP address (1 host up) scanned in 19.867 seconds [root@redhatserver root]# _</pre>
---	--

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Identificar el sistema operativo</h4> <p>xprobe2</p> <pre>libcap rpm -i libpcap-0.7.2-7.9.1.i386.rpm</pre> <pre>xprobe2 tar xvfz xprobe2-0.2.2.tar.gz cd xprobe2-0.2.2 ./configure make make install</pre>
---	--



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <p><i>Identificar el sistema operativo</i></p> <p>xprobe2</p> <pre>xprobe2 <IP> [-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.0.1. Module test failed [-] ping:udp_ping module: no closed/open UDP ports known on 192.168.0.1. Module test failed [-] No distance calculation. 192.168.0.1 appears to be dead or no ports known [+] Host: 192.168.0.1 is up (Guess probability: 25%) [+] Target: 192.168.0.1 is alive. Round-Trip Time: 0.01095 sec [+] Selected safe Round-Trip Time value is: 0.02198 sec [-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known) [+] Primary guess: [+] Host 192.168.0.1 Running OS: "FreeBSD 4.4" (Guess probability: 71%) [+] Other guesses: [+] Host 192.168.0.1 Running OS: "FreeBSD 4.5" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.6" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.6.2" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.7" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.8" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.9" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 4.10" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 5.0" (Guess probability: 71%) [+] Host 192.168.0.1 Running OS: "FreeBSD 5.1" (Guess probability: 71%) [+] Cleaning up scan engine [+] Modules deinitialized [+] Execution completed. [root@redhatserver root]#</pre>
---	---

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <p><i>Identificar la versión de los servicios</i></p> <p>amap</p> <pre>tar xfz amap-5.0.tar.gz cd amap-5.0 ./configure make make install</pre>
---	--



Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3> <h4>Identificar la versión de los servicios</h4> <p style="color: red;">amap</p> <pre>amap -bqv <IP> <puerto> Ejemplo: amap -bqv 172.16.2.250 80 TARGET PORT The target address and port(s) to scan (additional to -i) amap is a tool to identify application protocols on target ports. Usage hint: Options "-bqv" are recommended, add "-l" for fast/rush checks. [root@redhatserver amap-5.0]# amap -bqv 192.168.0.1 80 Using trigger file ./appdefs.trig ... loaded 23 triggers Using response file ./appdefs.resp ... loaded 309 responses Using trigger file ./appdefs.rpc ... loaded 458 triggers amap v5.0 (www.thc.org/thc-amap) started at 2005-05-01 22:19:29 - MAPPING mode Total amount of tasks to perform in plain connect mode: 17 Protocol on 192.168.0.1:80/tcp (by trigger http) matches http - banner: HTTP/1.1 404 Objeto no encontrado\r\nServer Microsoft-IIS/5.0\r\nDate Sun, 01 May 2005 2 03846 GMT\r\nContent-Type: text/html\r\nContent-Length: 116\r\n\r\n<html><head><ti ticle>Sitio no encontrado</title></head>\n<body>No hay ningn sitio Web en esta dir eccin. Protocol on 192.168.0.1:80/tcp (by trigger http) matches http - banner: HTTP /1.1 404 Objeto no encontrado\r\nServer Microsoft-IIS/5.0\r\nDate Sun, 01 May 20 05 203846 GMT\r\nContent-Type: text/html\r\nContent-Length: 116\r\n\r\n<html><head><ti ticle>Sitio no encontrado</title></head>\n<body>No hay ningn sitio Web en esta direccin. Waiting for timeout on 16 connections ... amap v5.0 finished at 2005-05-01 22:19:35 [root@redhatserver amap-5.0]# _</pre>
---	--

Contenido Introducción Localizar el objetivo Analizar el objetivo	<h3>Capítulo 2. Buscar un vector de ataque</h3>  <p>RETO</p> <div style="border: 2px solid red; padding: 10px; margin-top: 10px;"><p>Utiliza las herramientas descritas anteriormente para escanear los siguientes equipos:</p><ul style="list-style-type: none">•Equipos de la red interna (dirección automática NAT)•Equipo de la red interna 192.168.0.101/24•Un equipo externo</div>
---	--

Analista de Seguridad Informática

Capítulo 2. Buscar un vector de ataque

Capítulo 2. Buscar un vector de ataque

Contenido

- Introducción
- Localizar el objetivo
- Analizar el objetivo



CONTRAMEDIDAS

Para evitar que un ataque obtenga información de nuestra empresa debemos tomar las siguientes medidas

- Cortar todo el tráfico ICMP
- Utilizar una correcta arquitectura de red



