

Seguridad de Sistemas

Clase 4: Enumeración

Contenidos



- Conocer las principales técnicas de Enumeración para obtención de información
- Conocer los principales servicios utilizados para Enumeración
- Conocer las principales contramedidas para evitar ataques de Enumeración

Introducción

- **Enumeración:**
- Es la técnica a través de la cual se obtiene información específica de los servicios objetivo, a través de consultas.
- La información que se obtiene en esta etapa es:
 - Directorios compartidos
 - Usuarios y grupos
 - Nombres de servidores o hosts
 - Configuración de servicios
 - Tablas de rutas
 - Aplicaciones instaladas

Enumeración

	TCP/UDP 53 DNS Zone Transfer		UDP 161 Simple Network Management protocol (SNMP)
	TCP/UDP 135 Microsoft RPC Endpoint Mapper		TCP/UDP 389 Lightweight Directory Access Protocol (LDAP)
	UDP 137 NetBIOS Name Service (NBNS)		TCP/UDP 3268 Global Catalog Service
	TCP 139 NetBIOS Session Service (SMB over NetBIOS)		TCP 25 Simple Mail Transfer Protocol (SMTP)
	TCP/UDP 445 SMB over TCP (Direct Host)		TCP/UDP 162 SNMP Trap

Enumeración

- Utilizando NetBios:
- El comando para ejecutar esta función es:
 - nbtstat -A ipdestino
 - A continuación se muestra un ejemplo

```
C:\Users\Jgomez>nbtstat -A 172.24.100.64

VirtualBox Host-Only Network:
Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

Host no encontrado.

Ethernet:
Dirección IP del nodo: [172.24.100.137] Id. de ámbito : []

Tabla de nombres de equipos remotos de NetBIOS

  Nombre                               Tipo      Estado
-----
DUOC-2IA1RF7K3J<00>                   único     Registrado
GRUPO_TRABAJO <00>                     Grupo     Registrado
DUOC-2IA1RF7K3J<03>                   único     Registrado
DUOC-2IA1RF7K3J<20>                   único     Registrado
GRUPO_TRABAJO <1E>                     Grupo     Registrado
JAIME GOMEZ <03>                      único     Registrado

Dirección MAC = 08-00-27-DF-F0-10
```

Enumeración

- Herramientas para Enumeración vía NetBios
- SuperScan de McAfee
 - Entrega información detallada de los servicios que se están ejecutando el servidor remoto, usuarios, política de contraseñas
 - https://www.freewarefiles.com/SuperScan_program_18765.html

```
Total Users: 4

--- 1 ---
Admin "Administrador"
Full Name:      ""
System Comment: "Cuenta integrada para la
administración del equipo o dominio"
User Comment:   ""
Last logon:     Fri Apr 26 16:47:50 2013 (270 days
ago)
Password expires: Never
Password changed: 545 days ago
Locked out:     No
Disabled:       Yes
Number of logons: 14
Bad password count: 0

--- 2 ---
User "HomeGroupUser$"
Full Name:      "HomeGroupUser$"
System Comment: "Cuenta integrada para el acceso de
grupo en el hogar al equipo"
User Comment:   ""
Last logon:     Never
Password expires: Never
Password changed: 20 days ago
Locked out:     No
```

Enumeración

- **Enumeración de cuentas de usuario**
- PsTools: corresponde a una serie de herramientas desarrolladas por Microsoft para obtener información de usuarios vía NetBIOS
 - PsExec - execute processes remotely
 - PsFile - shows files opened remotely
 - PsGetSid - display the SID of a computer or a user
 - PsInfo - list information about a system
 - PsPing - measure network performance
 - PsKill - kill processes by name or process ID
 - PsList - list detailed information about processes

Enumeración

- Ejemplo

```
PsService v2.20 - Service information and configuration utility
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will
be unable to run.
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1   STOPPED
                               (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
                               (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

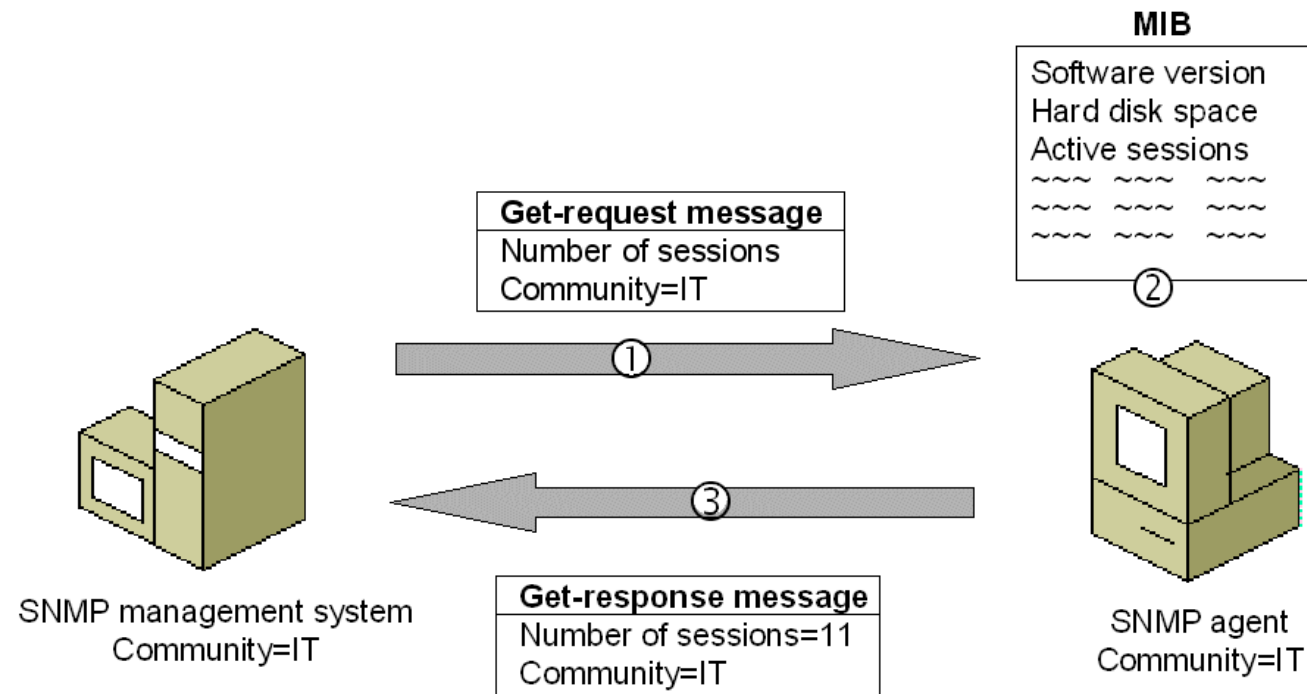
SERVICE_NAME: AppIDSvc
DISPLAY_NAME: Application Identity
Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.
        GROUP               : ProfSvc_Group
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1   STOPPED
                               (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0
```


Enumeración vía SNMP

- SNMP (Simple Network Management Protocol) es un servicio que se utiliza para interrogar a sistemas y obtener variables de ellos, fundamentalmente para monitoreo y supervisión.
- Tiene dos modos de operación, lectura y escritura; el primero, generalmente se configura en modo público sin contraseña
- La principal información que se puede obtener a través de esta técnica es:
 - Tablas de ruta
 - Estadísticas de trafico
 - Información del dispositivo

Enumeración vía SNMP

- Operación del protocolo SNMP:



- Comando para realizar enumeración vía SNMP
 - `nmap -sU -p 161 ipdestino`

Enumeración vía SNMP

- Ejemplo

[*] Routing information:

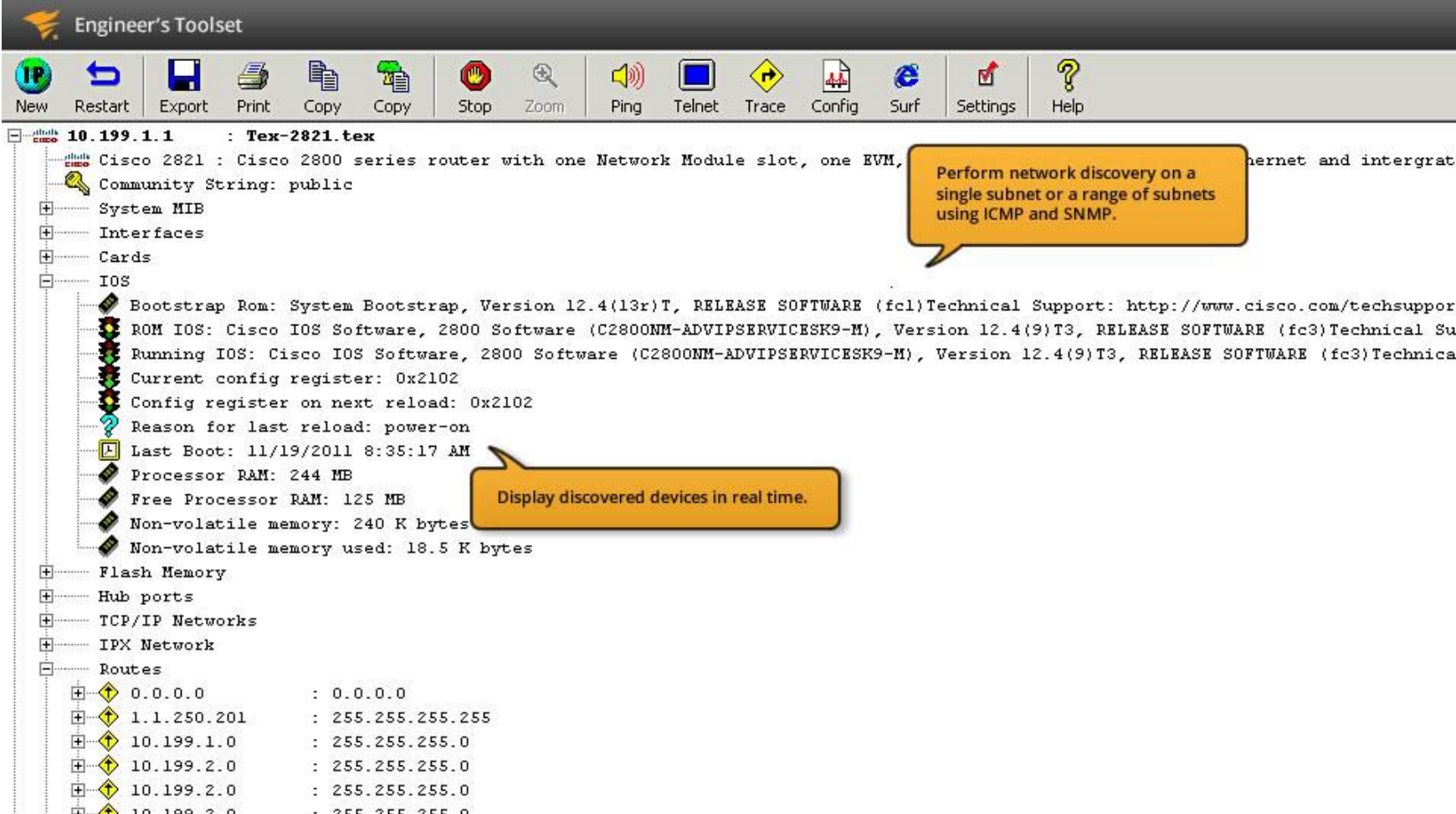
Destination	Next hop	Mask	Metric
0.0.0.0	10.0.2.1	0.0.0.0	10
10.0.2.0	10.0.2.10	255.255.255.0	266
10.0.2.10	10.0.2.10	255.255.255.255	266
10.0.2.255	10.0.2.10	255.255.255.255	266
127.0.0.0	127.0.0.1	255.0.0.0	306
127.0.0.1	127.0.0.1	255.255.255.255	306
127.255.255.255	127.0.0.1	255.255.255.255	306
224.0.0.0	127.0.0.1	240.0.0.0	306
255.255.255.255	127.0.0.1	255.255.255.255	306

[*] TCP connections and listening ports:

Local address	Local port	Remote address	Remote port	State
0.0.0.0	135	0.0.0.0	0	listen
0.0.0.0	49152	0.0.0.0	0	listen

Enumeración vía SNMP

- Ejemplo:



The screenshot displays the 'Engineer's Toolset' interface. The main window shows the configuration and status of a Cisco 2821 router. The left sidebar lists various system components like System MIB, Interfaces, Cards, and IOS. The main pane shows detailed information about the router, including its software version (12.4(9)T3), memory (244 MB), and boot time (11/19/2011 8:35:17 AM). A table at the bottom lists the discovered routes.

Engineer's Toolset

10.199.1.1 : Tex-2821.tex

Cisco 2821 : Cisco 2800 series router with one Network Module slot, one EVM, and one Network Module.

Community String: public

System MIB

Interfaces

Cards

IOS

Bootstrap Rom: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1) Technical Support: <http://www.cisco.com/techsupport>

ROM IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3) Technical Support: <http://www.cisco.com/techsupport>

Running IOS: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T3, RELEASE SOFTWARE (fc3) Technical Support: <http://www.cisco.com/techsupport>

Current config register: 0x2102

Config register on next reload: 0x2102

Reason for last reload: power-on

Last Boot: 11/19/2011 8:35:17 AM

Processor RAM: 244 MB

Free Processor RAM: 125 MB

Non-volatile memory: 240 K bytes

Non-volatile memory used: 18.5 K bytes

Flash Memory

Hub ports

TCP/IP Networks

IPX Network

Routes

0.0.0.0	: 0.0.0.0
1.1.250.201	: 255.255.255.255
10.199.1.0	: 255.255.255.0
10.199.2.0	: 255.255.255.0
10.199.2.0	: 255.255.255.0
10.199.2.0	: 255.255.255.0

Perform network discovery on a single subnet or a range of subnets using ICMP and SNMP.

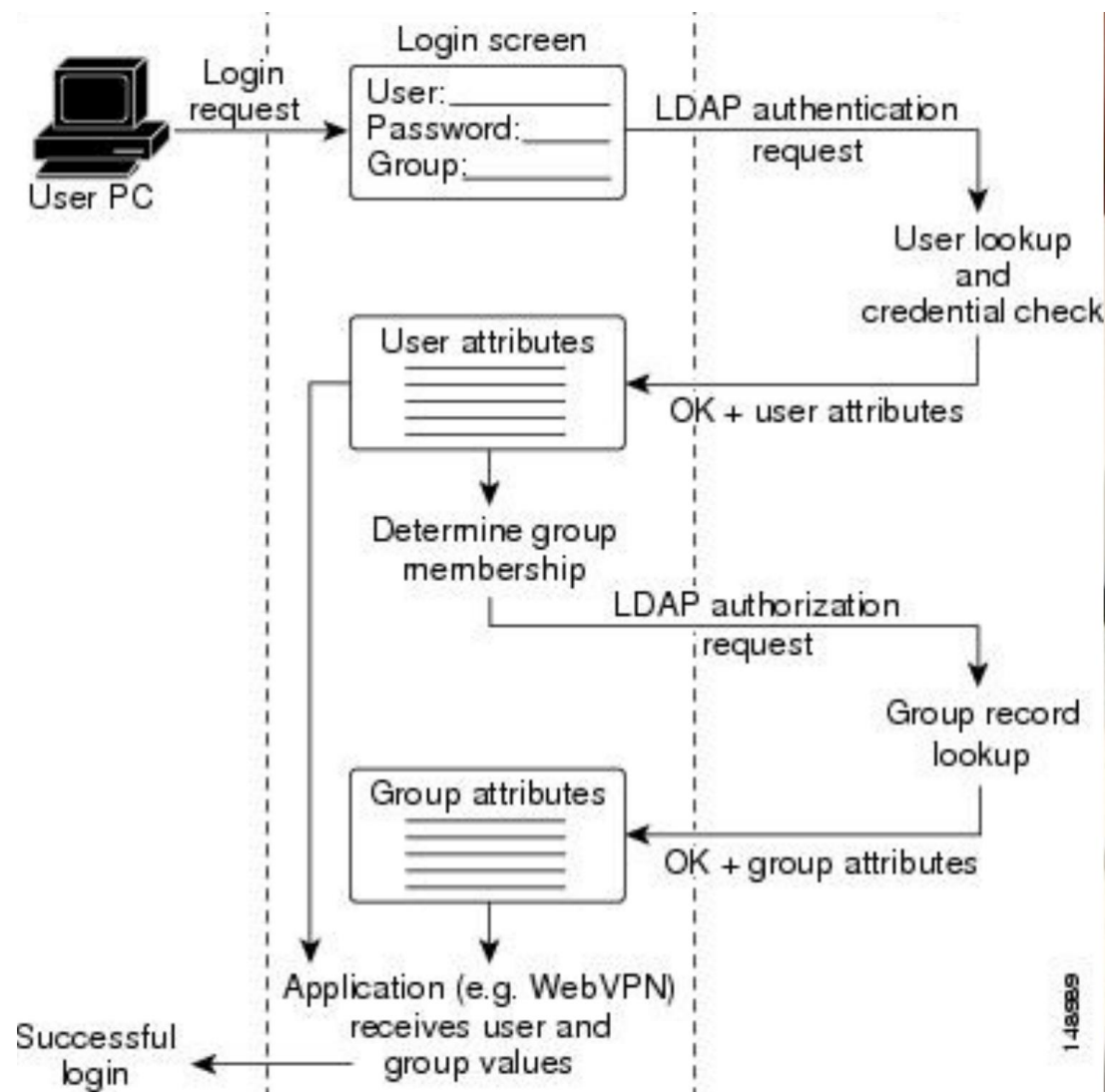
Display discovered devices in real time.

Enumeración vía LDAP



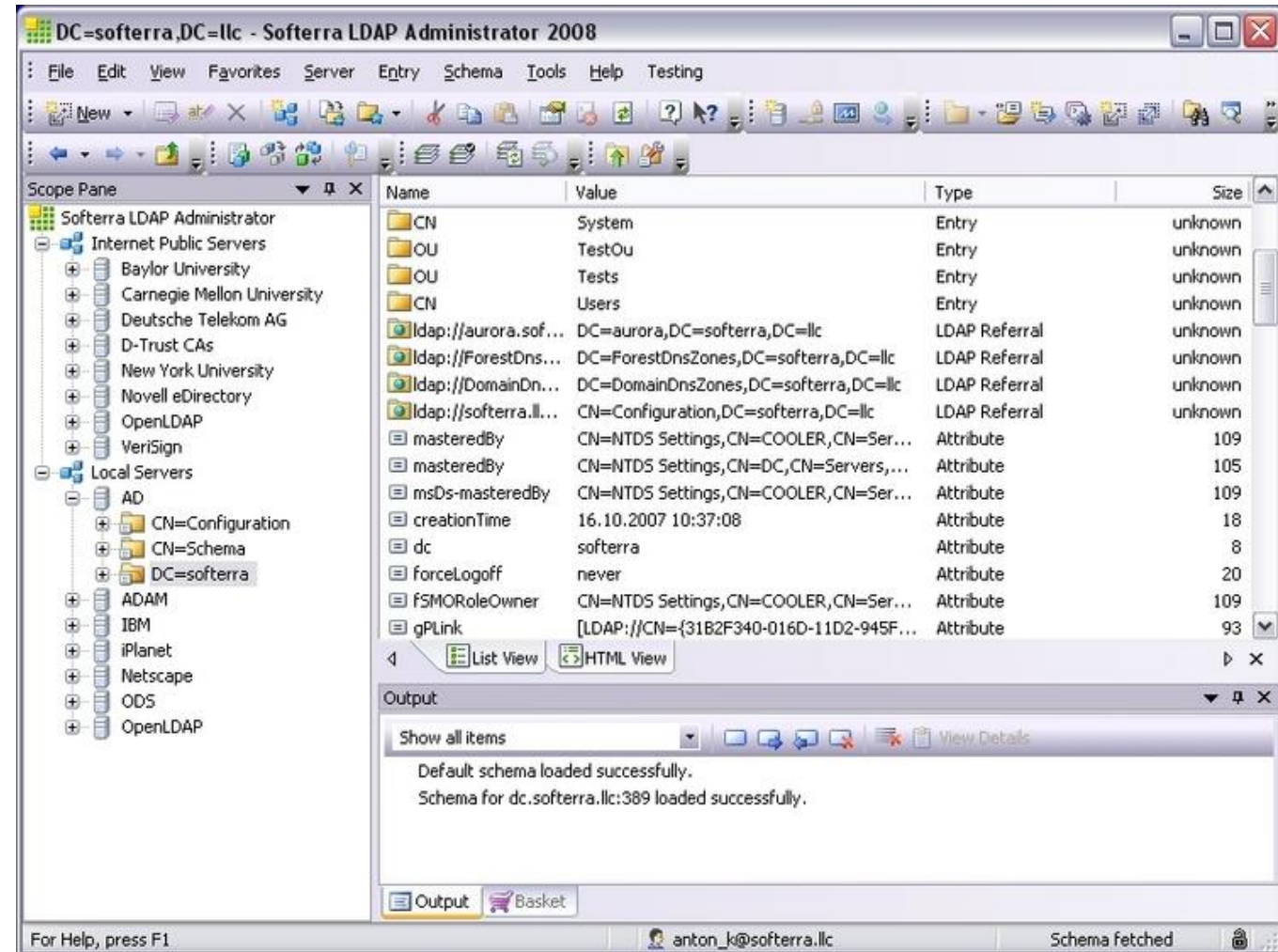
USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA



Enumeración vía LDAP

- LDAP Administrator



Enumeración vía SMTP

- El protocolo de envío de correos SMTP (Simple Mail Transfer Protocol) tiene una serie de comandos que pueden entregar información valiosa respecto de los usuarios del sistema
- Ejemplo:
 - VRFY: este comando permite validar usuarios en el sistema
 - EXPN: este comando entrega la dirección de uso del sistema
 - RCPT TO: este comando define al recipiente del mensaje

Enumeración vía SMTP

- Ejemplo de enumeración utilizando servicio SMTP

```
root@kali:~# nc -nv 10.0.2.60 25
(UNKNOWN) [10.0.2.60] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY msfadmin
252 2.0.0 msfadmin
VRFY pepito
550 5.1.1 <pepito>: Recipient address rejected: User unknown in local recipient
table
```

Esta operación se puede automatizar fácilmente, permitiendo obtener el listado de los usuarios válidos de un servidor de correo

Enumeración en sistemas Linux

- Dado la gran cantidad de servicios que es posible encontrar en un servidor Linux, se ha creado una herramienta que permite obtener el máximo de información.
- Ejemplo de uso de enum4linux

```
Server          Comment
-----
Workgroup       Master
-----
WORKGROUP      METASPLOITABLE

[+] Attempting to map shares on 10.0.2.60
//10.0.2.60/print$ Mapping: DENIED, Listing: N/A
//10.0.2.60/tmp Mapping: OK, Listing: OK
//10.0.2.60/opt Mapping: DENIED, Listing: N/A
//10.0.2.60/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//10.0.2.60/ADMIN$ Mapping: DENIED, Listing: N/A
```

Enumeración en sistemas Linux

- Para la enumeración interna de Sistemas Linux existe una herramienta llamada LinEnum, que permite obtener información de archivos y procesos del servidor con fallas conocidas de implementación y configuración.
- <https://github.com/rebootuser/LinEnum>
- System Information:
 - Hostname
 - Networking details:
 - Current IP
 - Default route details
 - DNS server information

Enumeración en sistemas Linux

- Ejemplo LinEnum

```
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.2 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic

[-] Hostname:
poloboxe Shell
Cheat Sheet | ...

### USER/GROUP #####
[-] Current user/group info:
uid=1002(user3) gid=1002(user3) groups=1002(user3)

[-] Users that have previously logged onto the system:
Username      Port      From      Latest
user3         pts/0     10.8.3.50  Mon May  4 23:36:24 -0400 2020
user8         pts/0     192.168.43.232  Mon Mar  2 10:33:59 -0500 2020

[-] Who else is logged on:
23:49:15 up 15 min,  1 user,  load average: 0.16, 0.13, 0.12
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU WHAT
user3     pts/0    10.8.3.50  23:36    3.00s  0.56s  0.00s /bin/bash ./LinEnum.sh
```

Enumeración de VPN

- Es posible realizar enumeración sobre servidores VPN los cuales pueden entregar información sensible tales como algoritmos de cifrado o algoritmos de hashing utilizados.
- Para comprobar que el servidor VPN esta activo
 - # nmap -sU -p 500
- Para realizar la enumeración
 - # ike-scan -M IP_server
 - URL=<https://github.com/royhills/ike-scan>

Enumeración de VPN

```
root@jeff:~# ike-scan 192.168.59.101 -M -A --id=groupnamedoesnotexit
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.59.101 Aggressive Mode Handshake returned
  HDR=(CKY-R=f58f20186b435cf1)
  SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
  KeyExchange(128 bytes)
  Nonce(20 bytes)
  ID(Type=ID_IPV4_ADDR, Value=192.168.59.101)
  Hash(16 bytes)
  VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
  VID=09002689dfd6b712 (XAUTH)
  VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
  VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator)

Ending ike-scan 1.9: 1 hosts scanned in 0.116 seconds (8.64 hosts/sec). 1 returned handshake; 0
returned notify
```


Enumeración VoIP

- Es posible obtener el listado de anexos activos, su configuración y datos de usuarios

```
[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1.
0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, R
EFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620 1
.0.4.33", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
```

Enumeración RPC

- RPC (Remote Procedure Call) es un programa que utiliza una computadora para ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambas. El protocolo que se utiliza para esta llamada es un gran avance sobre los sockets de Internet usados hasta el momento. De esta manera el programador no tenía que estar pendiente de las comunicaciones.
- Las RPC son muy utilizadas dentro de la comunicación cliente-servidor. Siendo el cliente el que inicia el proceso solicitando al servidor que ejecute cierto procedimiento o función y enviando este de vuelta el resultado de dicha operación al cliente

Enumeración RPC

```
root@kali:~# nmap -f -sV 192.168.0.10

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-04 13:53 EST
Nmap scan report for 192.168.0.10
Host is up (0.00034s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49156/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:90:2E:D4 (Oracle VirtualBox virtual NIC)
Service Info: Host: CHRIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.72 seconds
root@kali:~#
```


Enumeración RPC

nstdb - NetScanTools® Pro 11.90.1

File Edit Accessibility View IPv6 Help

Welcome

Automated Tools

Manual Tools (all)

ARP

ARP Cache

ARP Ping

ARP Scan

ARP Scan (MAC Scan)

Cache Forensics

Favorite Tools

Active Discovery Tools

Passive Discovery Tools

DNS Tools



Packet Level Tools

External Tools

Application Info

Manual Tools - ARP Scan (MAC Scan)

Use this tool to find all active IPv4 devices on your subnet.

IPv4  IPv6 

Ready

Do Arp Scan

Stop

Scan Delay Time (ms)

20

Packets sent per IP

3

☒ Resolve IPs

☒ Include Local I/F Info

Defaults

Jump To Dupe IP Scan

Network Interface

Ethernet (192.168.0.162) - Realtek PCIe GBE Family Controller

Starting IPv4 Address

192 . 168 . 0 . 1

Ending IPv4 Address

192 . 168 . 0 . 254


Add Note

Jump To Automated

Reports

☒ Add to Favorites

ARP Scanner Response Summary



1: Response, 9

2: +Other Local I/F, 1

3: No Response, 245

IPv4 Ad...	MAC Address	I/F Manufacturer	Hostname	Notes or Comments
192.168...	70-F1-96-...	Actiontec Electronics, Inc	?	Router
192.168...	00-16-B6-...	Cisco-Linksys, LLC	?	VOIP Box
192.168...	FC-3F-DB-...	Hewlett Packard		HP color laser printer/fax/copier
192.168...	00-30-48-...	Super Micro Computer, Inc.		Server in rack in closet
192.168...	24-E9-B3-...	Cisco Systems, Inc	?	RV180 router
192.168...	30-85-A9-...	ASUSTek COMPUTER INC.		computer Win 10
192.168...	04-A1-51-...	NETGEAR	?	Netgear switch - main switch
192.168...	00-25-61-...	ProCurve Networking by HP	?	HP ProCurve 2520
192.168...	00-1A-70-...	Cisco-Linksys, LLC	?	SRW224G4 switch
192.168...	78-FE-3D-...	Juniper Networks	?	Juniper EX2200 switch

For Help, press F1

CAP NUM SCRL

Contraseñas por defecto

- Hoy en día existen muchos sistemas que utilizan sus contraseñas por defecto, principalmente por razones administrativas, principalmente en los dispositivos de comunicaciones como switches y routers.
- Sitio que contiene contraseñas por defecto de los principales sistemas:
 - <https://cirt.net/passwords>

Default Passwords



	2Wire, Inc.	360 Systems
3COM	3M	Accelerated Networks

Contraseñas por defecto

- Para NMAP existen una serie de scripts que permiten obtener las contraseñas por defecto de diferentes aplicaciones

```
root@kali:~# nmap -sV --script auth 10.0.2.60
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-30 01:23 UTC
Nmap scan report for 10.0.2.60
Host is up (0.021s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
| mysql-empty-password:
|_  root account has empty password
| mysql-users:
|  debian-sys-maint
|  guest
|_  root
```

Enumeración web

- **Directorios:**
- Muchas aplicaciones web que puedes encontrar en Internet hoy en día pueden tener vulnerabilidades y estrategias de ataque que pueden ser explotadas por algún atacante que quiere el rol de administrador en tu servidor o simplemente quiere acceder a datos confidenciales en él.
- A través de este método, puedes encontrar fallas de seguridad serias en tu sitio web, como la disponibilidad de carpetas que se deben eliminar una vez que el proyecto haya sido finalizado, por ejemplo en herramientas como WordPress, PrestaShop, etc., y por lo tanto, podrás encontrar una solución para ello.

Enumeración web

- Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://prakharpasad.com:443/

Scan Information Results - List View: Dirs: 59 Files: 58 Results - Tree View Errors: 57

Type	Found	Response	Size
Dir	/	200	9246
Dir	/about/	200	664
Dir	/rss/	200	663
Dir	/login/	302	670
Dir	/security/	200	664
File	/cdn-cgi/l/email-protection	200	381
File	/rss	200	595
File	/rss/index.php	302	644
File	/rss/images.php	302	645
Dir	/rss/images/	302	668
Dir	/rss/index/	302	668
Dir	/rss/download/	302	668
File	/rss/2006.php	302	643
Dir	/rss/2006/	302	670

Current speed: 1 requests/sec (Select and right click for more options)

Average speed: (T) 10, (C) 1 requests/sec

Parse Queue Size: 0

Total Requests: 2006/9795735

Time To Finish: 113 Days

Current number of running threads: 20

Change

Program paused! /rss/09/privacy.php

Enumeración web

- **Archivos:**
- Hoy en día se publican una gran cantidad de archivos en aplicaciones web, no siempre con las medidas de seguridad necesarias.
- Para esto es relevante realizar un análisis de los documentos publicados, validar que no tengan información sensible o confidencial y que exista filtración de datos a través de los metadatos.
- FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Enumeración web

Eleven paths - FOCA (final version) 3.4

Project Report Tools Options TaskList Plugins About

FOCA

Custom search

Search engines: ☒ Google ☒ Bing ☐ Exalead All None

Extensions: ☒ doc ☒ xls ☒ ppsx ☒ sxc ☒ ppt ☒ docx ☒ xlsx ☒ sxi ☒ pps ☒ pptx ☒ sxw ☒ odt

Search All

Id	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
0	pdf	https://latch.elevenpaths.com/www/public/documents/...	•	02/09/2019 23:34:22	1,47 MB	•	02/09/2019 23:36:19
1	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:23	297,06 KB	•	02/09/2019 23:36:19
2	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:24	2,23 MB	•	31/05/2018 11:47:52
3	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:23	314,91 KB	•	02/09/2019 23:36:20
4	pdf	https://latch.elevenpaths.com/www/public/documents/...	•	02/09/2019 23:34:24	1,36 MB	•	02/09/2019 23:36:21
5	pdf	https://latch.elevenpaths.com/www/public/documents/...	•	02/09/2019 23:34:25	1,54 MB	•	02/09/2019 23:36:21
6	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:25	915,74 KB	•	02/09/2019 23:36:22
7	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:25	1,44 MB	•	02/09/2019 23:36:22
8	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:26	981,68 KB	•	02/09/2019 23:36:23
9	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:28	4,99 MB	•	02/09/2019 23:36:24
10	pdf	https://latch.elevenpaths.com/www/public/documents/...	•	02/09/2019 23:34:28	6,83 MB	•	07/02/2019 15:21:06
11	pdf	https://securityinnovationday.elevenpaths.com/public/d...	•	02/09/2019 23:34:28	3,47 MB	•	02/09/2019 23:36:27
12	pdf	http://www.elevenpaths.com/wp-content/uploads/2017...	•	02/09/2019 23:34:29	888,92 KB	•	02/09/2019 23:36:28
13	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:28	106,15 KB	•	02/09/2019 23:36:29
14	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:44	1,56 MB	•	31/05/2018 12:00:54
15	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:31	79 KB	•	02/09/2019 23:36:29
16	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:43	113,28 KB	•	02/09/2019 23:36:29
17	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:38	317,68 KB	•	02/09/2019 23:36:30
18	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:44	1,05 MB	•	02/09/2019 23:36:30
19	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:45	114,27 KB	•	02/09/2019 23:36:30
20	pdf	https://www.elevenpaths.com/wp-content/uploads/201...	•	02/09/2019 23:34:45	126,01 KB	•	02/09/2019 23:36:31

Time	Source	Severity	Message
23:36:37	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\Sinfonier_community_contest2015_EN.pdf
23:36:37	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\Cybersecurity_Beyond_Technology_Telef...
23:36:38	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\TrendReport_Vulnerabilidades_H1_2016...
23:36:38	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\Breaches_2016_T2_ES_v1.0.pdf
23:36:38	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\Breaches-2016-T3_EN_v1.0.pdf
23:36:39	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\SID2014_4_Nuevas_Tecnicas_Hacking...
23:36:39	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\ElevenPaths_HastenGroup_informative_n...
23:36:39	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\EULA_Metashield.pdf
23:37:12	MetadataSearch	low	Document metadata extracted: D:\Escritorio\Eleven Paths\EULA_Metashield.pdf

Conf Deactivate AutoScroll Clear Save log to File

Metadata analyzed!

Contramedidas

- **SNMP**
- Remover los agentes SNMP si no está siendo utilizados
- Permitir el acceso sólo a servidores autorizados
- Cambiar el nombre de las comunidades por defecto
- Utilizar SNMPv3, el cual permite cifrar las credenciales del usuario
- No permitir conexiones anónimas
- Filtrar los puertos de servicios a UDP 161

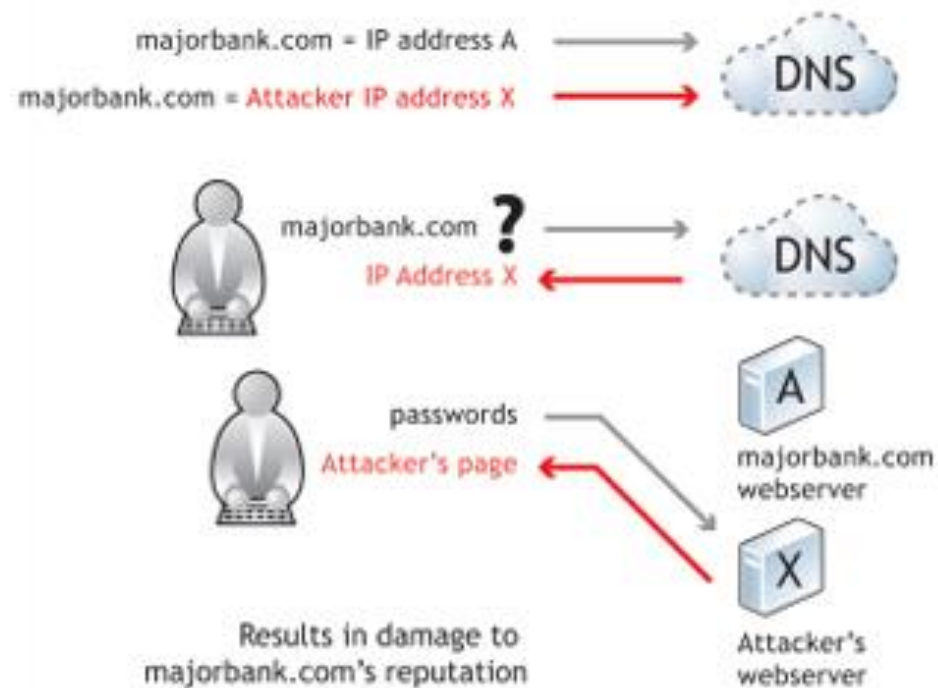
Contramedidas

- DNS
- Deshabilitar la transferencia de zona
- No publicar direcciones IP privadas en las zonas de DNS
- Separar los servicios de DNS interno y externo
- Utilizar DNSSec
- <https://www.csirt.gob.cl/reportes/an2-2020-15/>

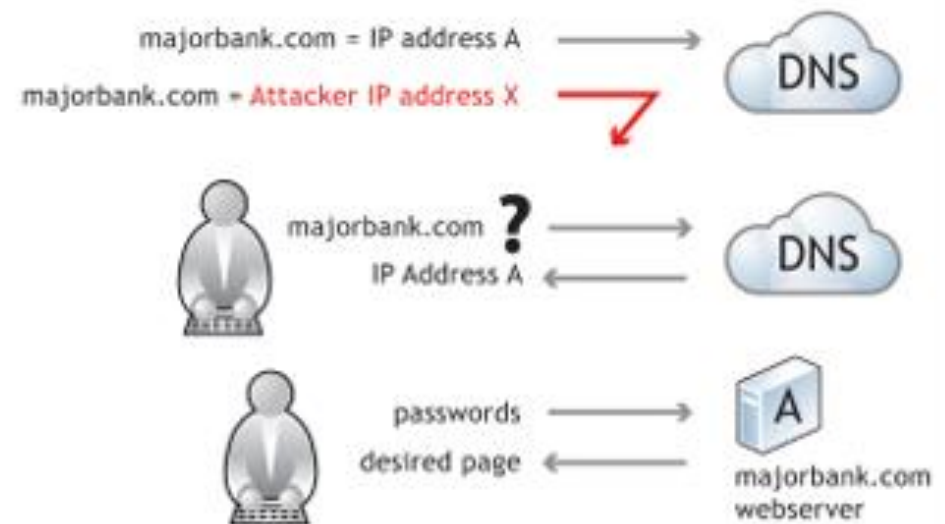
Contramedidas

- DNSSEC

Without DNSSEC



With DNSSEC



Contramedidas

- **SMTP**
- No recibir correos de remitentes desconocidos
- Utilizar solo gateways públicos para el envío y recepción de correos SMTP
- Deshabilitar el “open relay”
- Limitar el numero de conexiones entrantes para evitar ataques de Spaming
- Utilizar certificado digital para conexiones seguras

Contramedidas

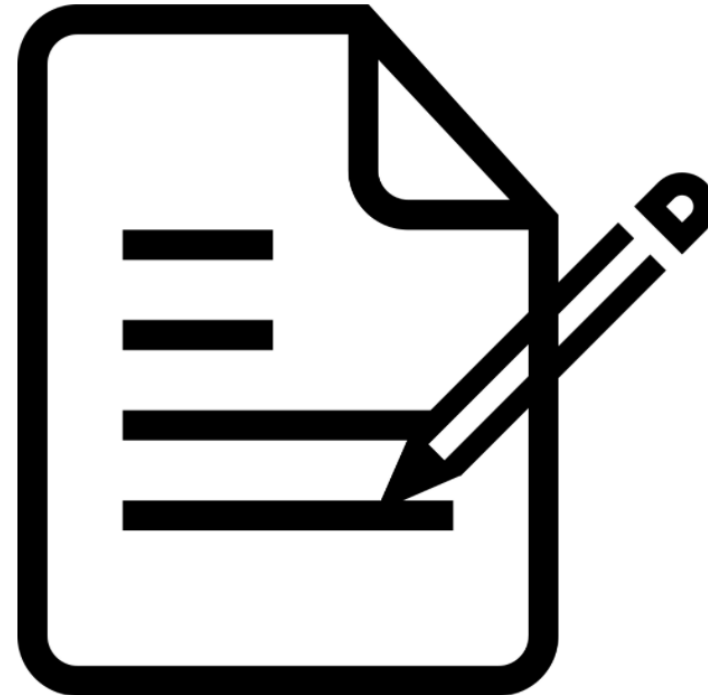
- **LDAP**
- Utilizar certificado digital para que el trafico viaje cifrado sobre SSL a través del puerto 636
- Utilizar un id de usuarios diferente al correo electrónico
- Restringir el acceso al servidor LDAP sólo a servicios autorizados

Contramedidas

- **SMB**
- Deshabilitar SMB en servidores DNS y Web
- Deshabilitar SMB de servidores que estén expuestos a Internet o redes públicas
- Restringir el acceso anónimo al servicio SMB
- Habilitar la característica de “SMB signing”

Resumen

- Servicios utilizados para Enumeración
 - NetBIOS
 - SNMP
 - LDAP
 - SMTP
 - Sistemas Linux
 - VPN
 - VoIP
 - RPC
- Contraseñas por defecto
- Enumeración web
- Contramedidas





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA