

Enumeraciones

Abril 2014

Introducción

- Una Enumeración es definida como un proceso de extraer nombre, dispositivos, recursos compartidos, etc.
- En la fase de enumeración el atacante crea conexiones activas a un sistema.
 - Se dirigen consultas para obtener más información.

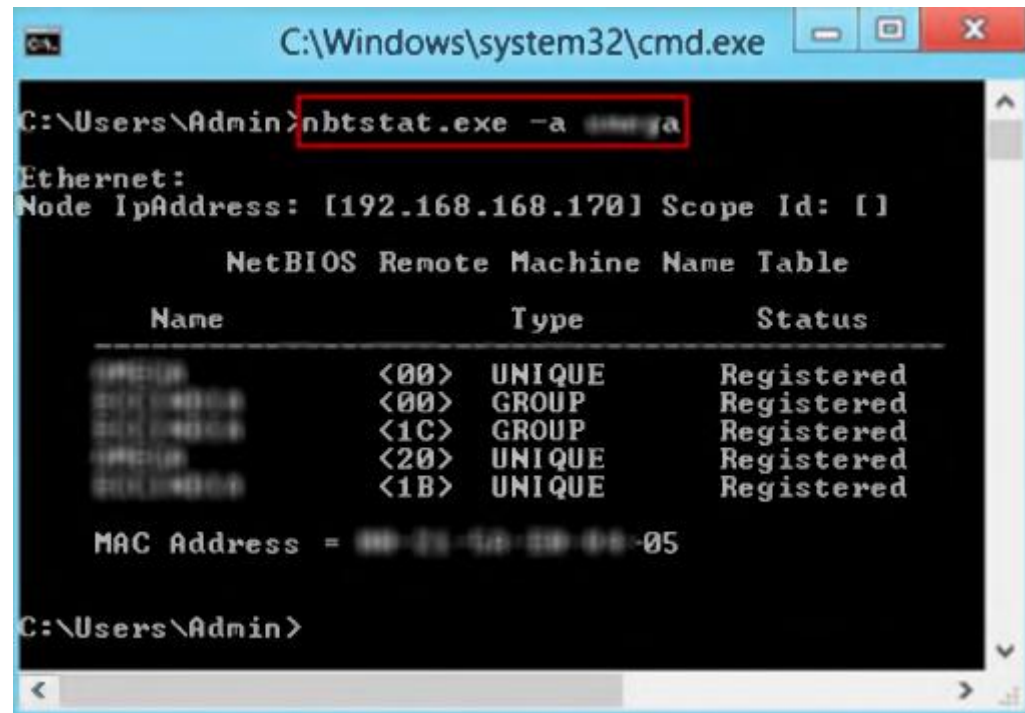
Características

- El usuario utiliza la información obtenida para identificar vulnerabilidades o puntos débiles.
- Las técnicas de Enumeración se utilizan en ambientes Intranet.

Información Enumerada

- Recursos de red compartidos
- Usuarios y grupos
- Tablas de enrutamiento
- Configuración de servicios
- Nombres de equipos
- Aplicaciones

Obteniendo información del NetBIOS



```
C:\Windows\system32\cmd.exe
C:\Users\Admin>nbtstat.exe -a omega
Ethernet:
Node IpAddress: [192.168.168.170] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    <00>                  UNIQUE          Registered
    <00>                  GROUP           Registered
    <1C>                  GROUP           Registered
    <20>                  UNIQUE          Registered
    <1B>                  UNIQUE          Registered

    MAC Address = 00-23-6E-00-00-05

C:\Users\Admin>
```

SuperScan

- Es una herramienta que utiliza el protocolo TCP, UDP para obtener información.
- Realiza un escaneo a través de hilos.
 - Resuelve nombres de equipos, reporta en HTML, soporta rango de IP's, etc.

IP	192.168.11.29
Hostname	[Unknown]
Netbios Name	SERVKEY-XPS
Workgroup/Domain	WORKGROUP

UDP Ports (1)			
137	NETBIOS Name Service		
UDP Port	Banner		
137	NETBIOS Name Service		
	MAC Address: C4:85:08:F1:8A:0B		
	NIC Vendor : Unknown		
	Netbios Name Table (4 names)		
	WORKGROUP	00 GROUP	Workstation service name
	SERVKEY-XPS	00 UNIQUE	Workstation service name
	SERVKEY-XPS	20 UNIQUE	Server services name
	WORKGROUP	1E GROUP	Group name

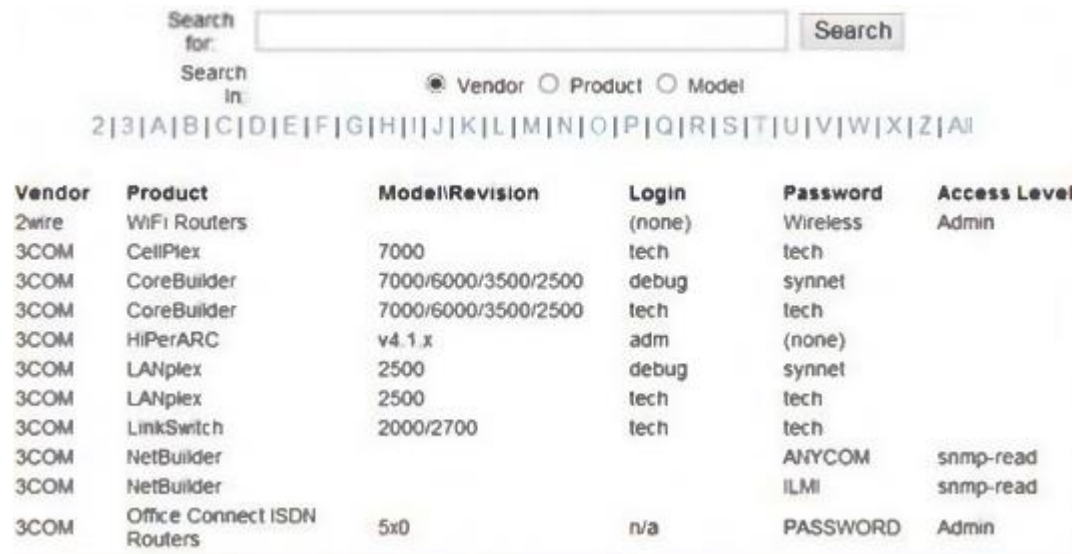
IP	192.168.11.40
Hostname	[Unknown]
Netbios Name	PRUEBAS-4BFCC1C
Workgroup/Domain	GRUPO_TRABAJO

UDP Ports (2)			
123	Network Time Protocol		
137	NETBIOS Name Service		
UDP Port	Banner		
137	NETBIOS Name Service		
	MAC Address: 08:00:27:9C:74:79		
	NIC Vendor : Pcs Comput		
	Netbios Name Table (6 names)		
	PRUEBAS-4BFCC1C	20 UNIQUE	Server services name
	PRUEBAS-4BFCC1C	00 UNIQUE	Workstation service name
	GRUPO_TRABAJO	00 GROUP	Workstation service name
	GRUPO_TRABAJO	1E GROUP	Group name
	GRUPO_TRABAJO	1D UNIQUE	Master browser name
	.._MSBROWSE_	01 GROUP	

IP	192.168.11.52
Hostname	[Unknown]

Enumeraciones – Contraseñas por Default

- Routers, Hubs, switches, access points muchas veces están configurados con las contraseñas por default.
 - <http://www.defaultpassword.com>



The screenshot shows the defaultpassword.com website. At the top, there is a search bar with the text "Search for:" and a "Search" button. Below the search bar, there are radio buttons for "Vendor", "Product", and "Model", with "Vendor" selected. Below the radio buttons, there is a list of letters from A to Z, with "A" selected. Below the list of letters, there is a table with the following columns: Vendor, Product, Model/Revision, Login, Password, and Access Level. The table contains 15 rows of data.

Vendor	Product	Model/Revision	Login	Password	Access Level
2wire	WiFi Routers		(none)	Wireless	Admin
3COM	CellPlex	7000	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	tech	tech	
3COM	HiPerARC	v4.1.x	adm	(none)	
3COM	LANplex	2500	debug	synnet	
3COM	LANplex	2500	tech	tech	
3COM	LinkSwitch	2000/2700	tech	tech	
3COM	NetBuilder			ANYCOM	snmp-read
3COM	NetBuilder			ILMI	snmp-read
3COM	Office Connect ISDN Routers	5x0	n/a	PASSWORD	Admin

Enumerando cuentas de usuario



Enumeraciones con LDAP



JXplorer

<http://www.jxplorer.org>



Active Directory Explorer

<http://technet.microsoft.com>



LDAP Admin Tool

<http://www.ldapsoft.com>



LDAP Administration Tool

<http://sourceforge.net>



LDAP Account Manager

<http://www.ldap-account-manager.org>



LDAP Search

<http://securityxploded.com>



LEX - The LDAP Explorer

<http://www.ldapexplorer.com>



**Active Directory Domain
Services Management Pack**

<http://www.microsoft.com>



LDAP Admin

<http://www.ldapadmin.org>



LDAP Browser/Editor

<http://www.novell.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited

Actividad

- Unix/Linux Enumeration
 - Enum4Linux
- SMTP Enumeration
 - NetScanTools

Metodología para explotar vulnerabilidades

