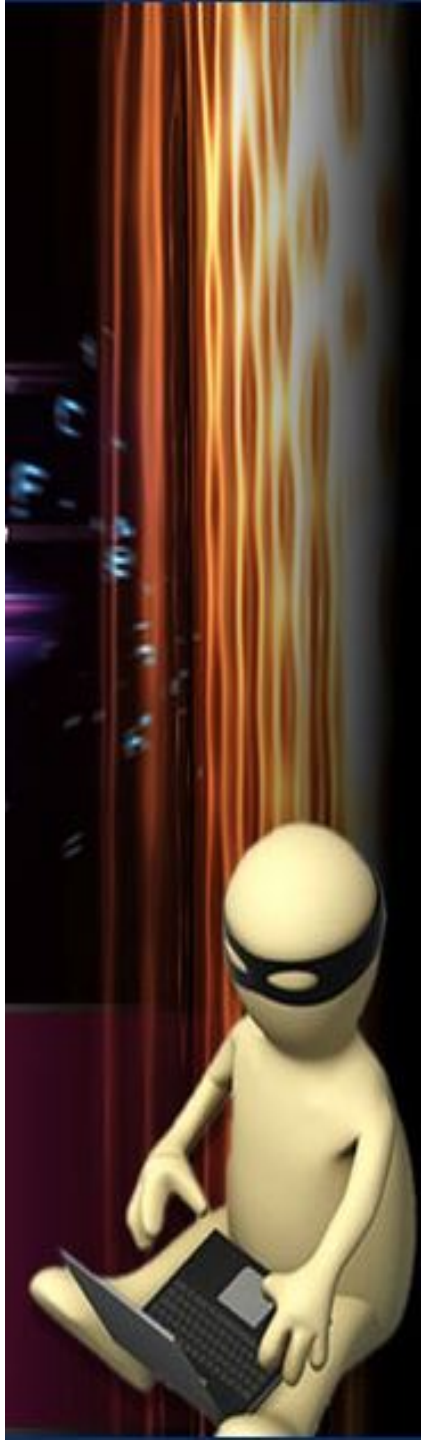
HACKING ÉTICO 101 3ra EDICIÓN

DIAPOSITIVAS ACOMPAÑANTES PARA INSTRUCTORES

www.KarinaAstudillo.com

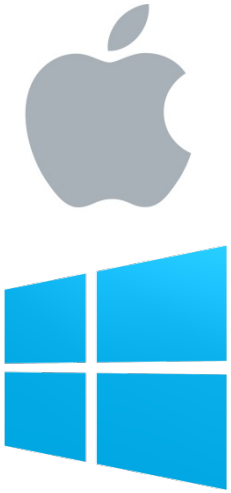


Escaneo

Clases de escaneo, estados de puertos, Nmap, analizadores de vulnerabilidades.

¿Qué es escanear?

- Escanear implica identificar los puertos abiertos en los hosts activos identificados en la fase previa.
- Incluye la detección del sistema operativo de los sistemas escaneados y de las aplicaciones asociadas a los puertos abiertos.



(*) Todas las marcas pertenecen a sus respectivos dueños.

Ping Sweepers

Ping Scanner Pro - registered

File Options Help

WinNet | Network Stats | Connections | Telnet | Port Scan | IP List | Routing table | Interfaces

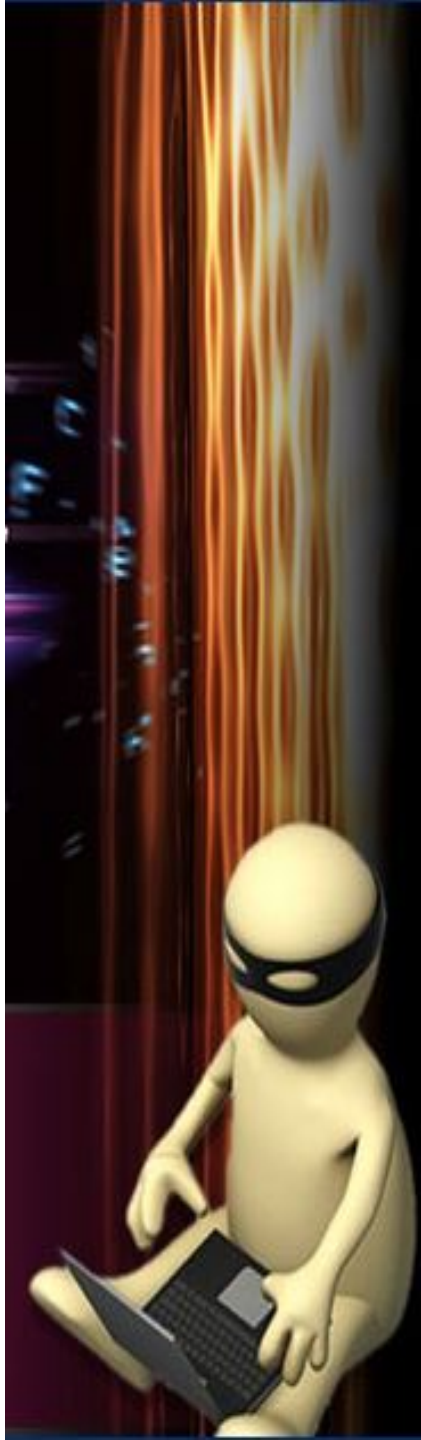
Ping | Multi Ping | Trace Route | MAC | DNS | Whois | IP Calculator | Finger | Troughput | NT Users

Start 2 122 53 60 Time Out 250 Start Scan Cancel Clear

End 2 122 54 60 Resolve ☑

IP	status	Time	Name
2 122.53.69	OK	194 ms.	[redacted]
2 122.53.70	OK	203 ms.	[redacted]
2 122.53.71	OK	210 ms.	[redacted]
2 122.53.72	OK	188 ms.	[redacted]
2 122.53.73	OK	195 ms.	[redacted]
2 122.53.74	OK	189 ms.	[redacted]
2 122.53.75	OK	189 ms.	No name found
2 122.53.76	OK	200 ms.	No name found
2 122.53.77	OK	201 ms.	[redacted]
2 122.53.78	OK	184 ms.	[redacted]
2 122.53.79	Late	334 ms.	No name found
2 122.53.80	OK	196 ms.	[redacted]
2 122.53.81	No answer	n/a	n/a
2 122.53.82	No answer	n/a	n/a
2 122.53.83	Late	711 ms.	[redacted].com
2 122.53.84	No answer	n/a	n/a

MultiPing canceled by user

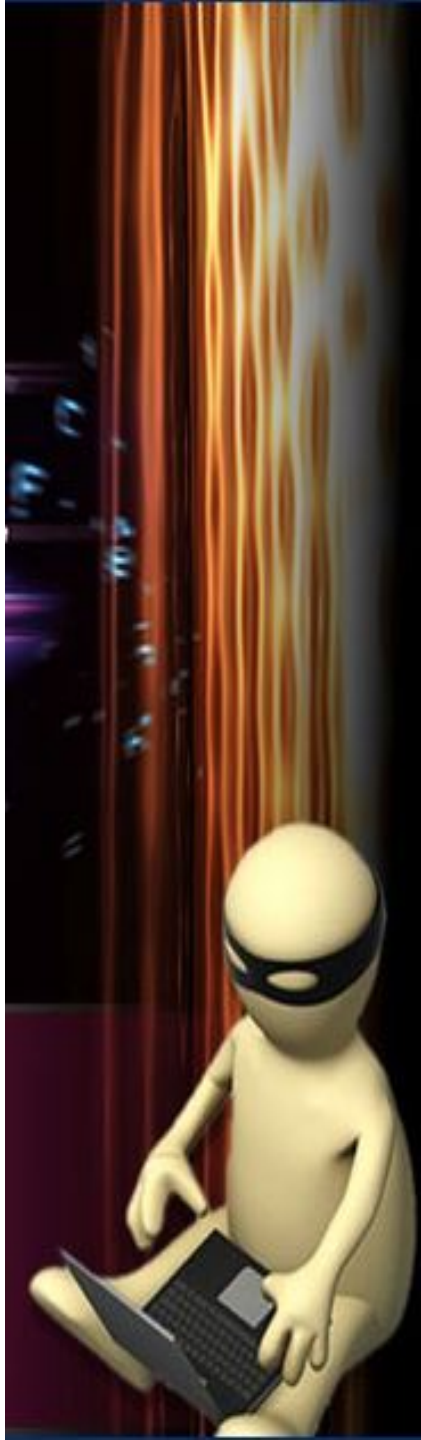


TCP Ping

C:\windows\system32\cmd.exe

```
C:\Users\Karina\Desktop>pingtcp.exe www.elixircorp.com 80
PingPort 1.0. TCP port access tester. http://sysadminblog.ru , http://xtelekom.ru

Reply from www.elixircorp.com:80 OK. Time=453ms
Reply from www.elixircorp.com:80 OK. Time=281ms
Reply from www.elixircorp.com:80 OK. Time=280ms
Reply from www.elixircorp.com:80 OK. Time=281ms
Reply from www.elixircorp.com:80 OK. Time=281ms
Reply from www.elixircorp.com:80 OK. Time=281ms
Reply from www.elixircorp.com:80 OK. Time=260ms
Reply from www.elixircorp.com:80 OK. Time=267ms
Reply from www.elixircorp.com:80 OK. Time=259ms
Reply from www.elixircorp.com:80 OK. Time=260ms
Reply from www.elixircorp.com:80 OK. Time=266ms
Reply from www.elixircorp.com:80 OK. Time=281ms
Reply from www.elixircorp.com:80 OK. Time=260ms
Reply from www.elixircorp.com:80 OK. Time=260ms
^C
C:\Users\Karina\Desktop>
```



Estados de puertos

•**Abierto:** un puerto en este estado está disponible y escuchando por conexiones hacia el servicio asociado en dicho puerto.

•**Cerrado:** por el contrario un puerto cerrado aunque es accesible, no tiene una aplicación o servicio asociado que responda a solicitudes de conexión.

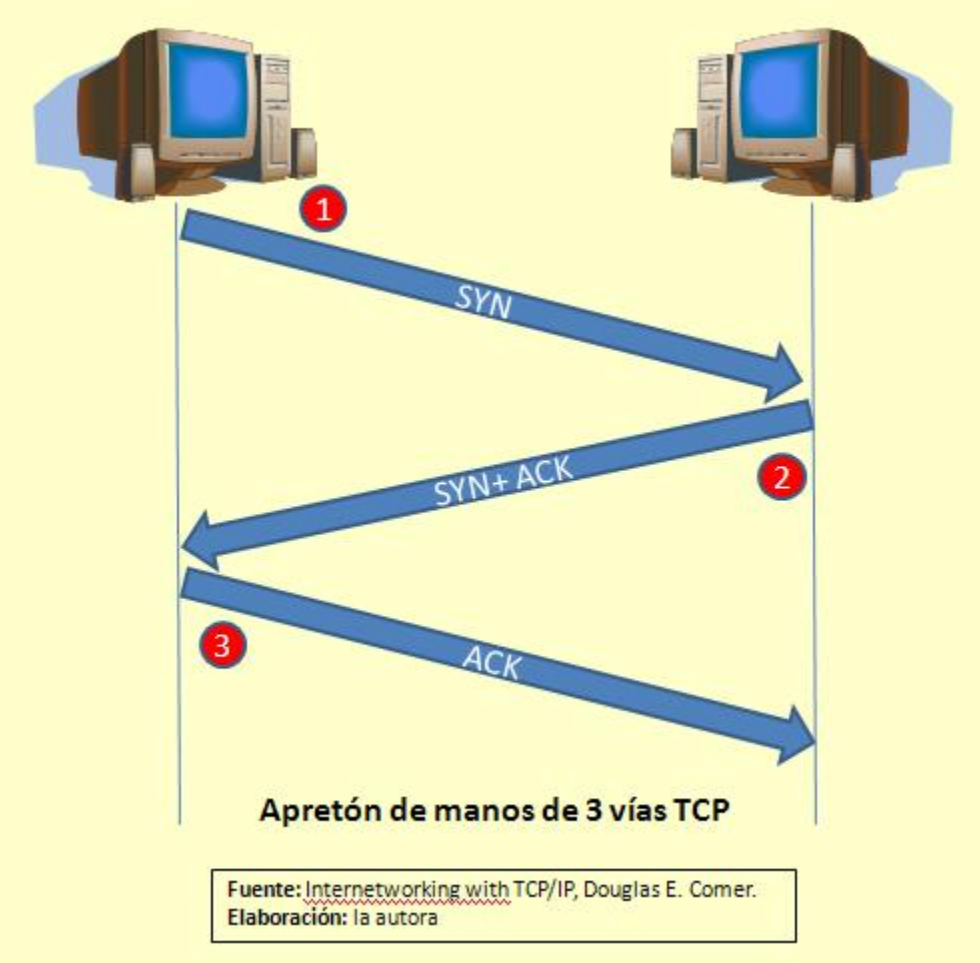
•**Filtrado:** un puerto filtrado no es posible de ser accesado porque existe un dispositivo filtrador de paquetes de por medio que impide al escáner determinar si dicho puerto está abierto o cerrado.

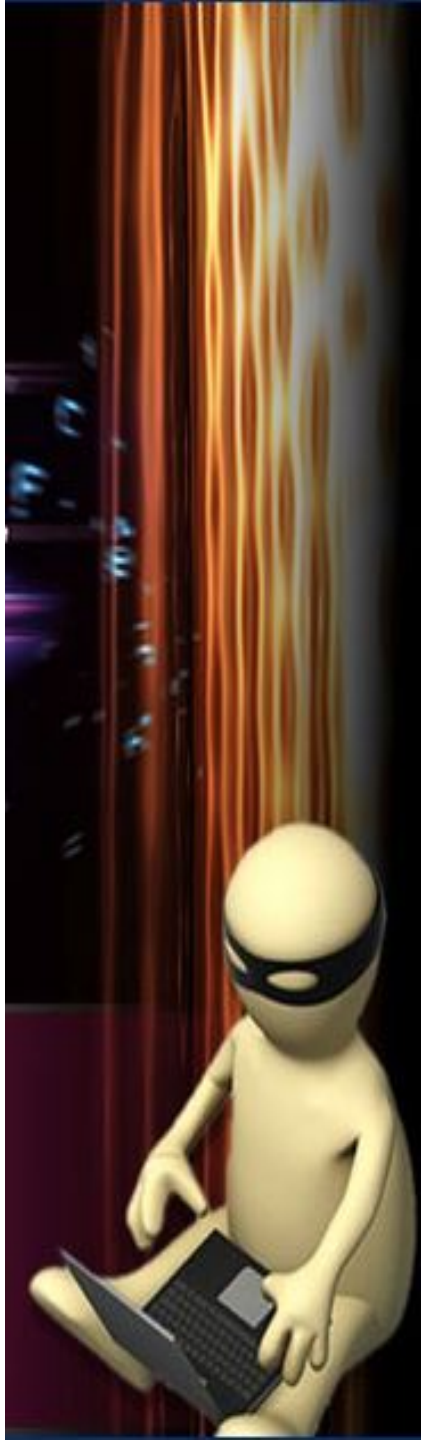
•**No-filtrado**: un puerto en este estado es accesible pero no puede determinarse a ciencia cierta si está abierto o cerrado. Este estado es específico de la técnica de escaneo ACK.

•**Abierto | Filtrado:** este es un estado ambiguo en el cual el escáner no pudo determinar si el puerto se encuentra abierto o filtrado y es factible de obtenerse cuando se usa una técnica de escaneo en la cual un puerto abierto puede no responder.

•**Cerrado | Filtrado:** se da cuando el escáner no puede concluir si el puerto está cerrado o filtrado.

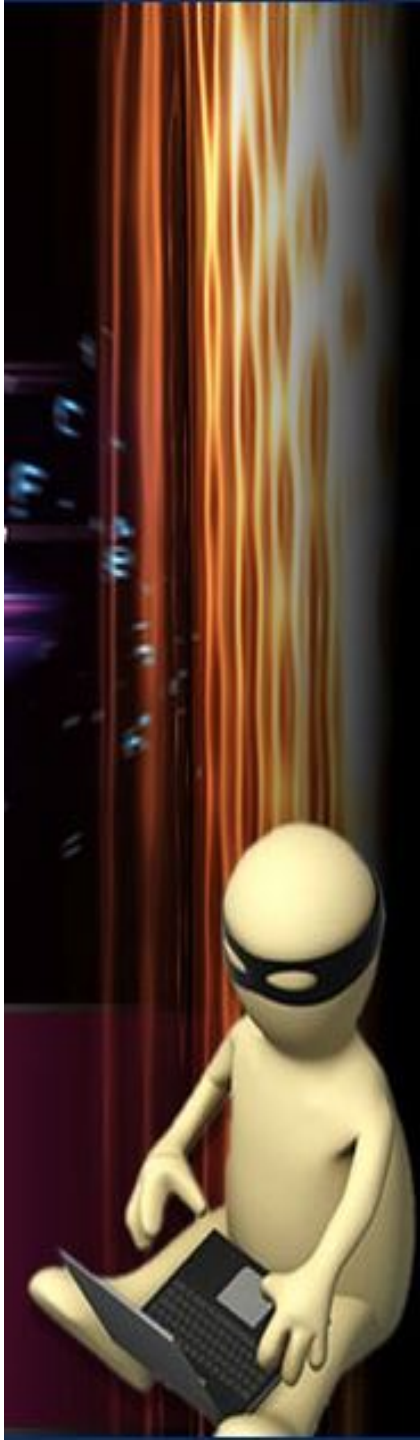
Three-way handshake TCP



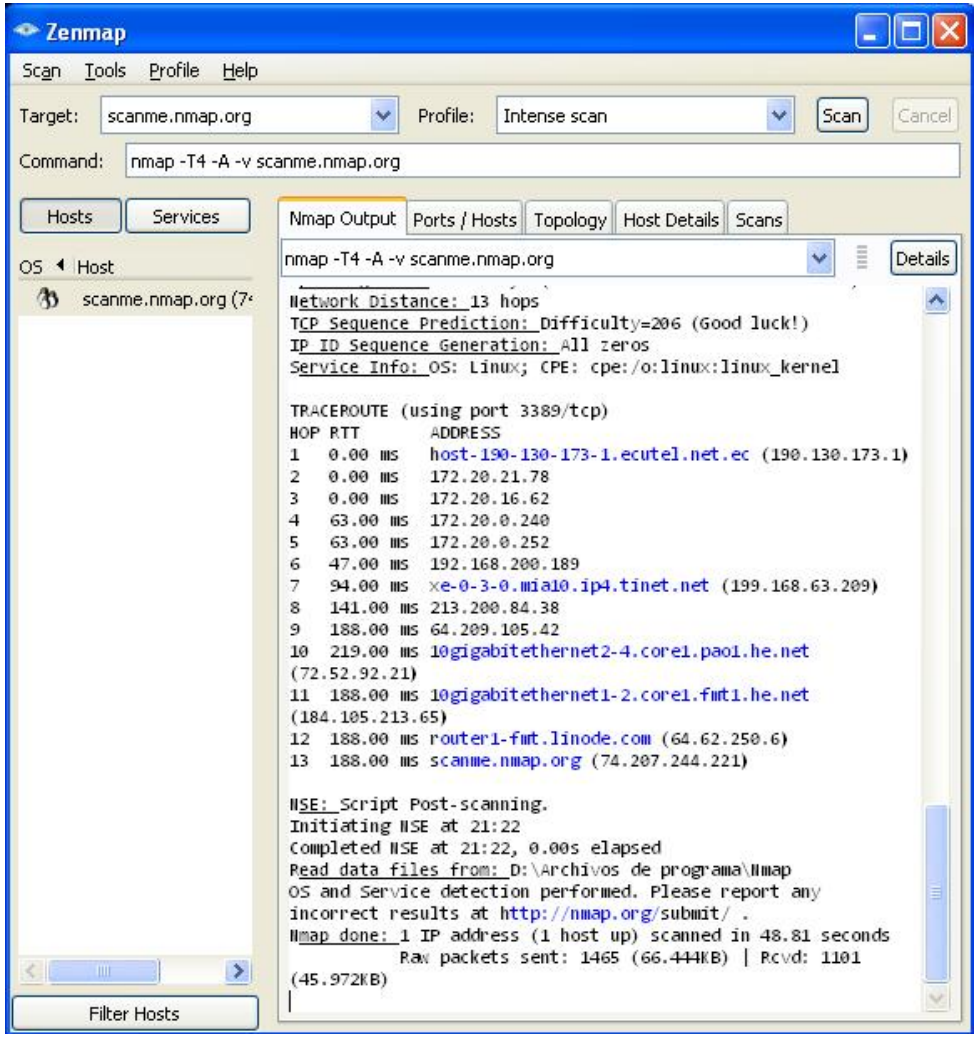


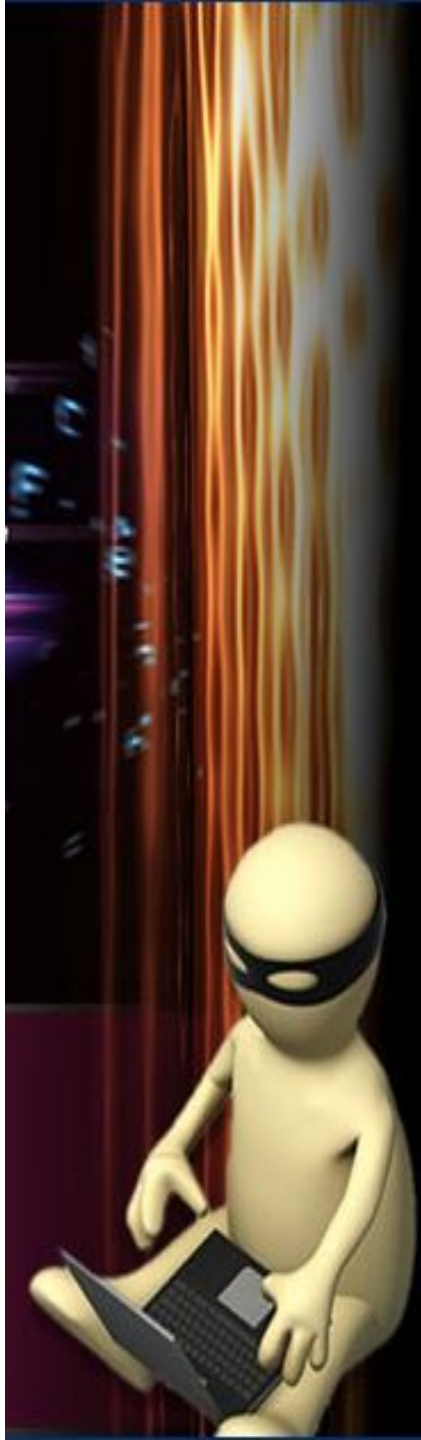
Técnicas de Escaneo

- Escaneo SYN o Half-Open
- Escaneo FULL o Connect-Scan
- Escaneo UDP
- Escaneos especiales (si RST cerrado):
  - Null Scan (flags off)
  - FIN Scan (FIN on)
  - XMas Scan (FIN + URG + PSH)
- Escaneo ACK (si RST no-filtrado)



Escáner de puertos NMAP





Sintaxis NMAP

nmap [tipo(s)_de_escaneo] [opciones] {red|host_objetivo}

Opciones:

-sn : ping scan
-sS : syn/half scan
-sT : tcp/connect scan
-sA : ack scan
-sN : null scan
-sU : udp scan
-sF : fin scan
-sX : xmas scan
-sV : detección de versión de servicios
-O : detección de sistema operativo
-T<0-5>: temporizador, el valor más alto es más rápido
-v : salida detallada

NMAP desde el CLI

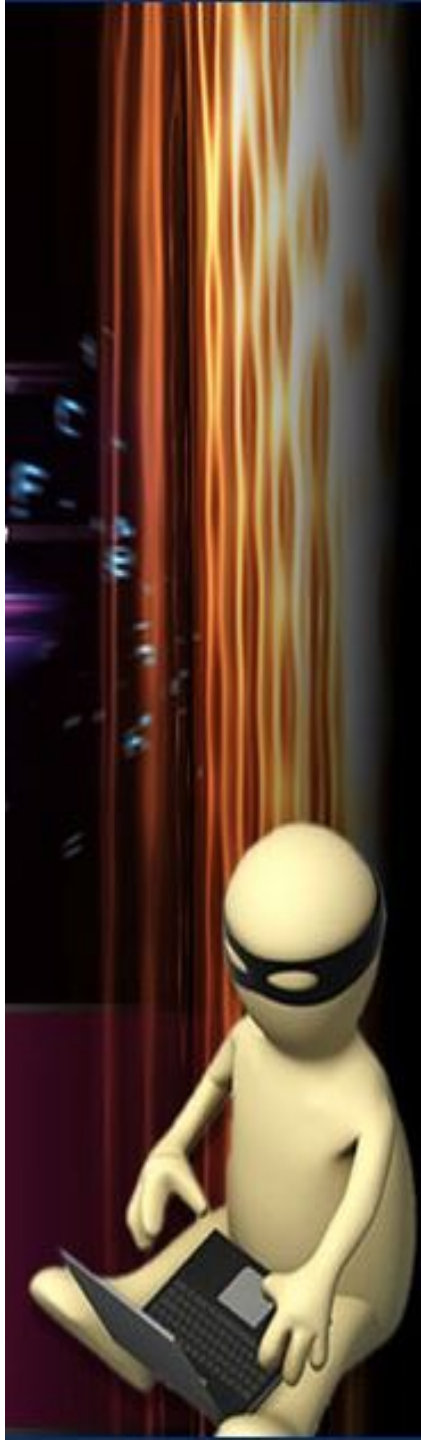
Símbolo del sistema

```
C:\Documents and Settings\Karina\Escritorio\Enumeration>nmap -O 192.168.91.133

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-09 20:56 Hora est. Or. (EE.UU.
 y Canadβ)
Nmap scan report for 192.168.91.133
Host is up (0.0000010s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1043/tcp open  boinc
1045/tcp open  fpitp
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:0C:29:97:FD:C4 (VMware)
Device type: general purpose
Running: Microsoft Windows XP¦2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::s
p1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds

C:\Documents and Settings\Karina\Escritorio\Enumeration>
```

Zenmap en acción

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org (7

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

scanme.nmap.org (74.207.244.221)

Host Status

State: up

Open ports: 4

Filtered ports: 1

Closed ports: 995

Scanned ports: 1000

Up time: 379757

Last boot: Mon Dec 10 11:52:48 2012

Addresses

IPv4: 74.207.244.221

IPv6: Not available

MAC: Not available

Hostnames

Name - Type: scanme.nmap.org - user

Name - Type: scanme.nmap.org - PTR

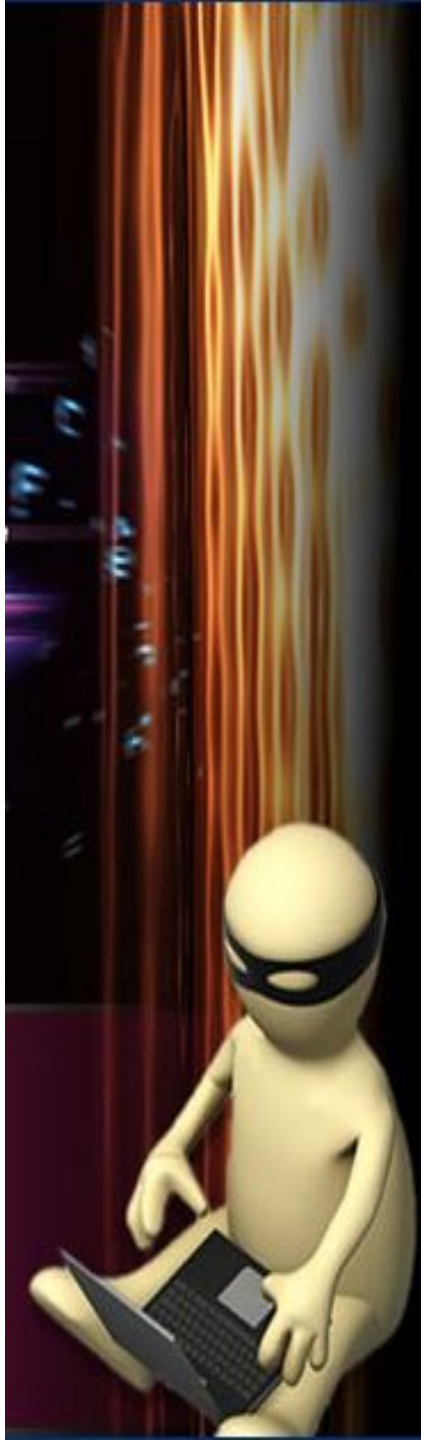
Operating System

Name: Linux 3.0

Accuracy: 9 %

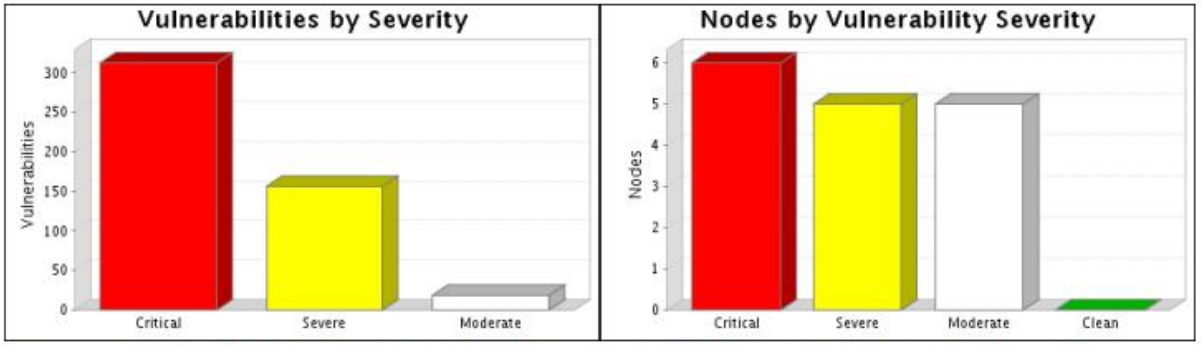
Ports used

OS Classes

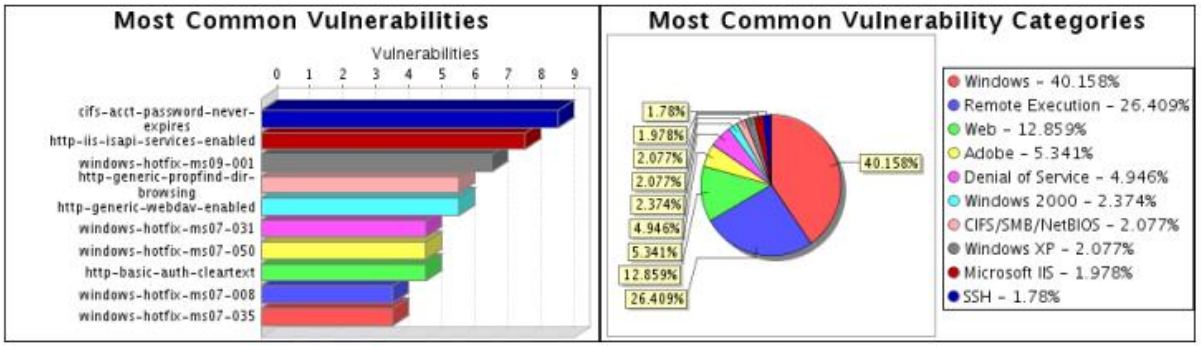


Analizadores de Vulnerabilidades

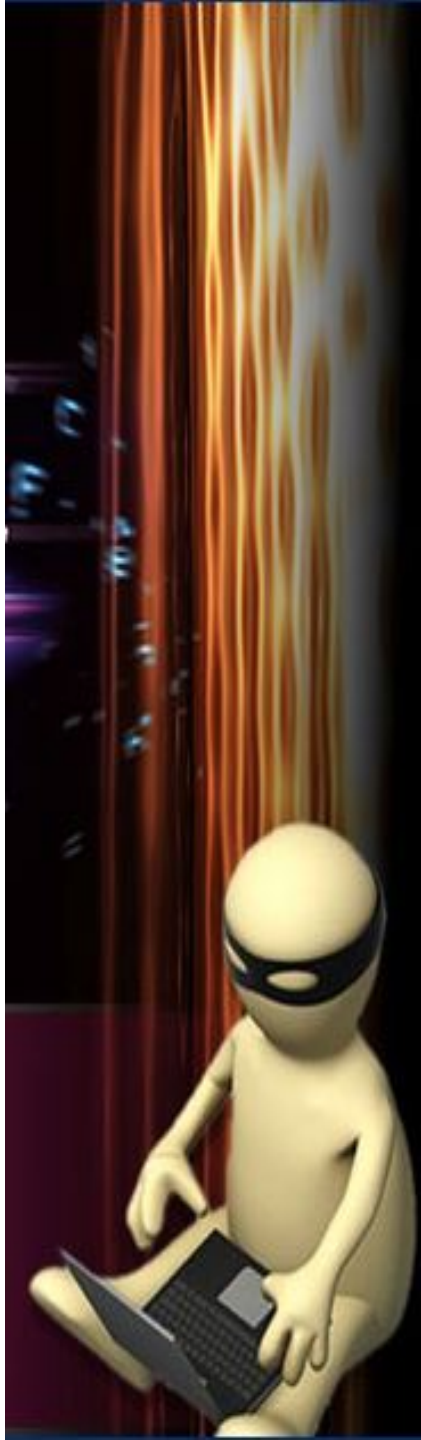
Audit Report



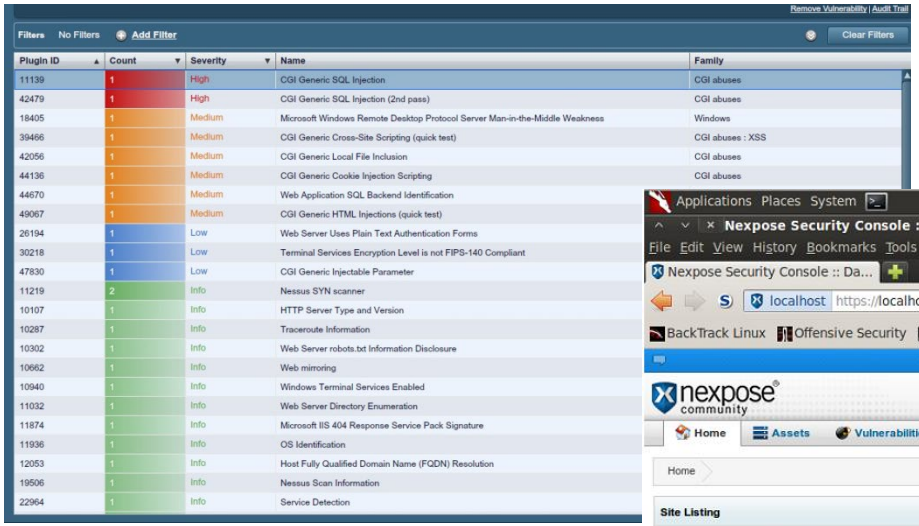
There were 489 vulnerabilities found during this scan. Of these, 313 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 157 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 19 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 6 of the systems, making them most susceptible to attack. 5 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 5 systems. No systems were free of vulnerabilities.

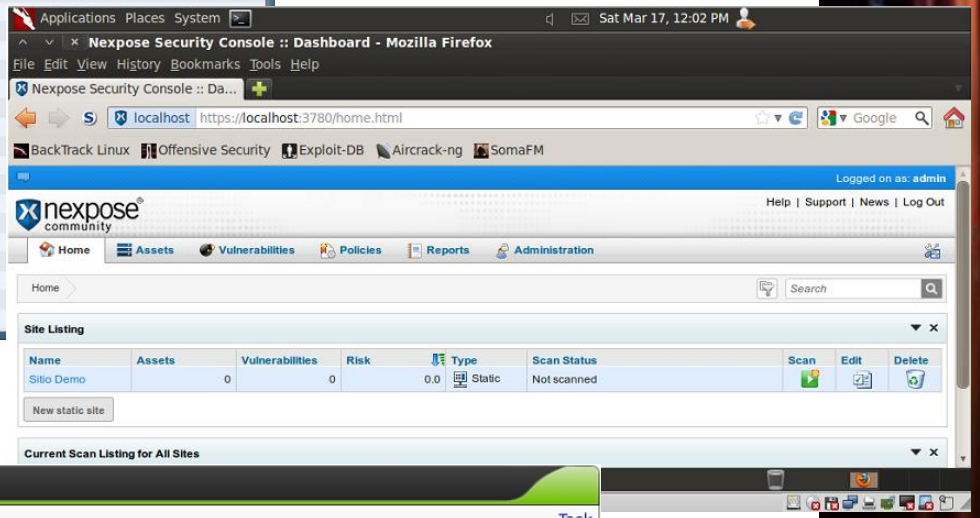


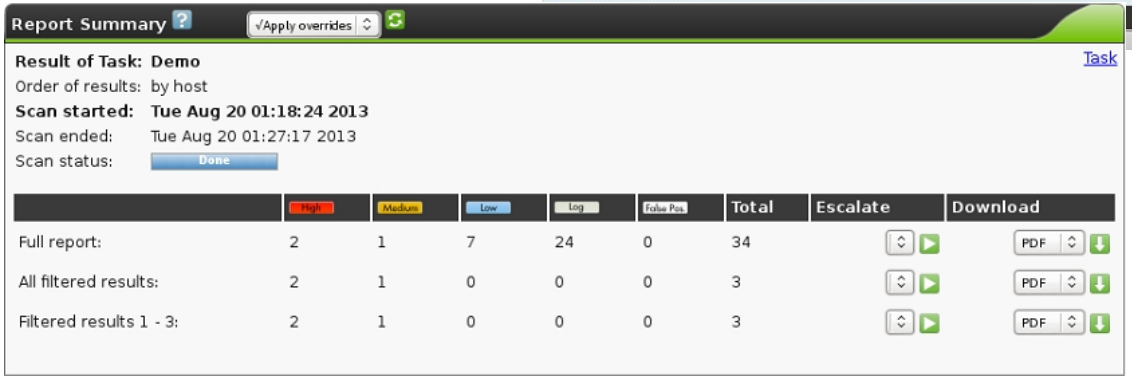
There were 9 occurrences of the cifs-acct-password-never-expires vulnerability, making it the most common vulnerability. There were 406 vulnerabilities in the Windows category, making it the most common vulnerability category.

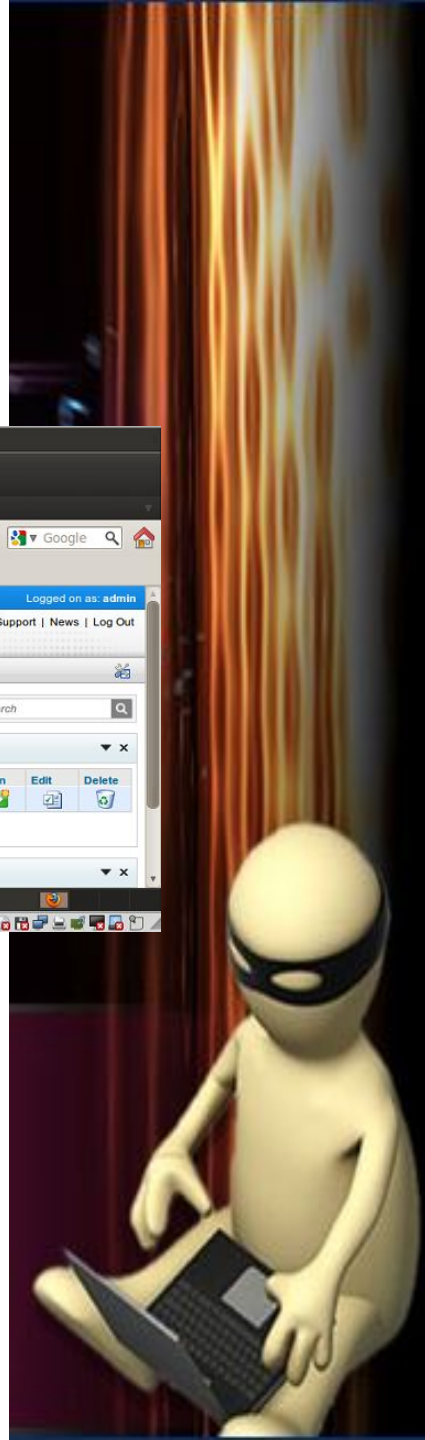


Analizadores Populares





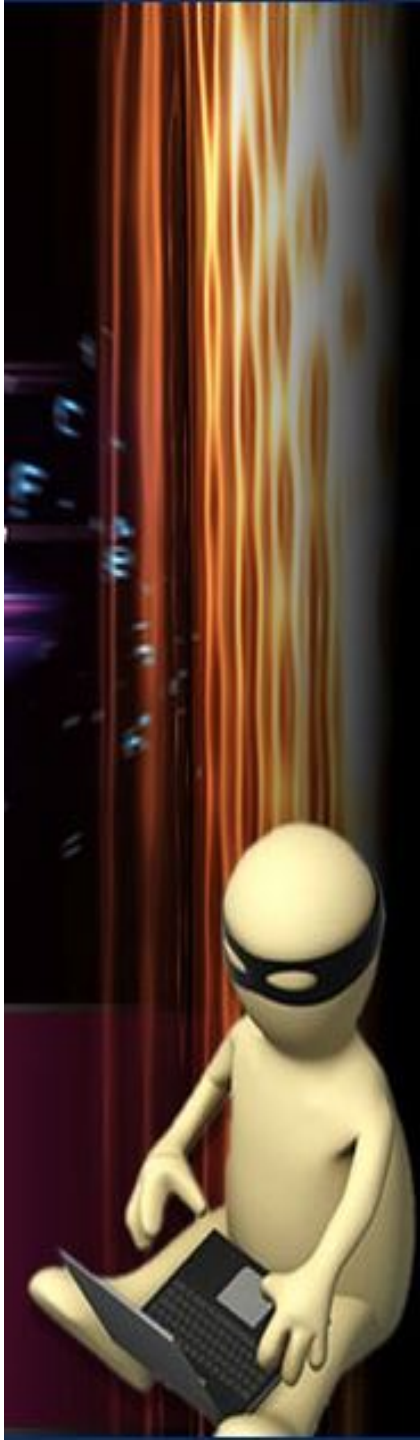




www.KarinaAstudillo.com

Medidas Defensivas

- Hardening
- Actualizaciones y subscripciones a foros
- Contratos de soporte al día
- Configuración correcta de Firewalls de Borde, sistemas IDS/IPS, LCE y monitoreo
- Auto análisis periódico



THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
JUSPAXAR
GOZAIMASHITA
EFCHARISTO
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
GRAZIE
MEHRBANI
MAAKE
KOMAPSUMNIDA
PALDIES
BOLZÏN
MERCI
BÏYAN
SHUKRIA
TINGKI
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGARATAM
HUI
GUI
HATUR
UNALCHÉESH
SPASIBO
DENKAUJA
NENACHALHYA
MERSI
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
DHANYABAAD
ANIHA
ATTO
SANCO
MERASTAWHY
GAEJTHO
LAH
AGUYJE
FAKAAUE
TAVTAPUCH
MEDAWAGSE
BAIKA