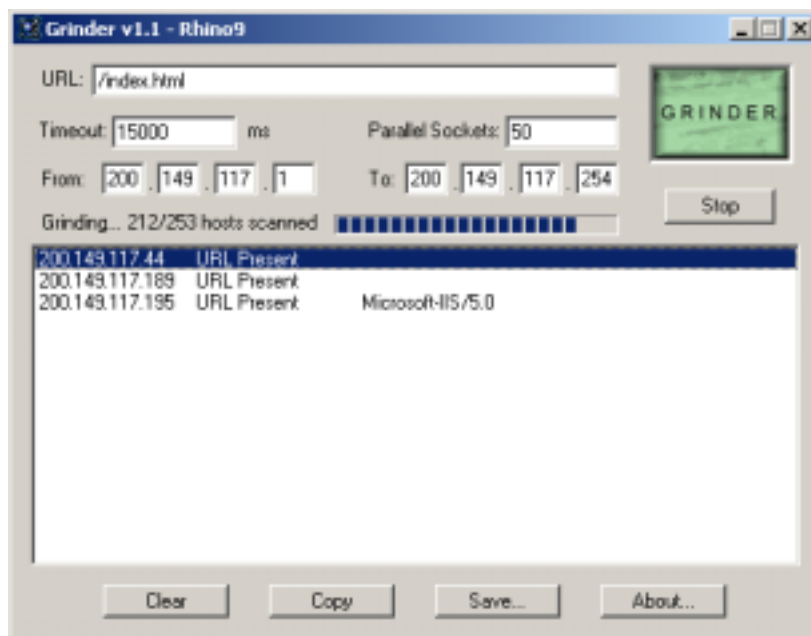


Práctica: 27. Detección del Sistema Operativo. Netcat, Grinder, chronicle (Por HxC Mods-Adm)

Con solo visitar la Web (si la tiene) ya podemos hacernos una idea del Sistema Operativo del servidor, no obstante podemos utilizar determinadas herramientas para detectar de un modo más fiable le S.O. en cuestión.

Grinder es una aplicación con la que podemos escanear una subred determinada en busca



Chronicle es una herramienta simila

Otra herramienta útil puedes ser nuestro versátil NetCat, ya sabes que esta es la herramienta de los “mil usos”. Netcat puede extraer las cabeceras de un servidor Web y mostrar el tipo de Servidor con un tanto por ciento elevado de acierto.

Siguiendo con el ejemplo anterior, podremos escribir esto:

```
Símbolo del sistema
C:\>nc -vv 200.149.117.195 80
dial tcp 200.149.117.195:80 [200.149.117.195] 80 <http> open
GET /index.html HTTP/1.1
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 03 Feb 2003 17:02:43 GMT
Content-Type: text/html
Content-Length: 0?

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>sent 13, rcvd 224: NOTSOCK
C:\>_
```

Como verás el servidor remoto responde “a las claras” que se trata de un IIS, por tanto estaremos casi seguros de que se trata de un Windows 2000/NT. Después de la orden `nc ip.remota 80` pulsa dos veces enter. También puedes usar `telnet ip.del.equipo 80` y dos veces enter.

En próximos capítulos encontraremos mejores utilidades para esto, espera a que lleguemos al escaneo de puertos.