

VERIFICACIÓN DE SEGURIDAD BÁSICA EN LA RED LOCAL.

Una buena práctica en nuestra empresa es la verificación de la seguridad de nuestra red y para ello proponemos dos comprobaciones simples, podemos llevar a cabo las mismas desde nuestro PC equipado con Windows.

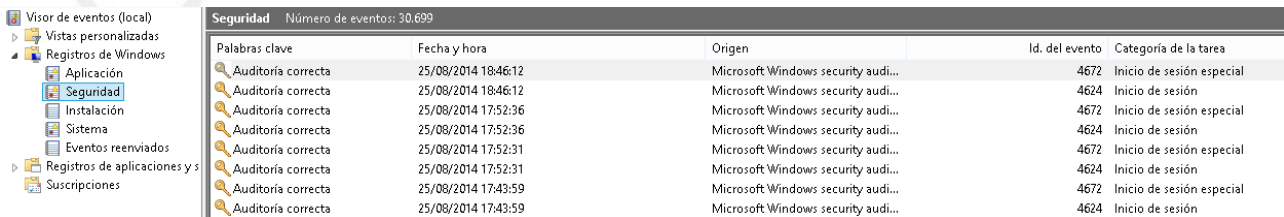
1º Control de Acceso.

¿Hay alguien intentando entrar en mi equipo y yo no lo sé?

Pues bien, para responder a esto lo mejor es fijarse en la lista de accesos del visor de sucesos de Windows. Para ello pulsar la tecla Windows + R y escribir Eventvwr.msc en la ventana que aparece.

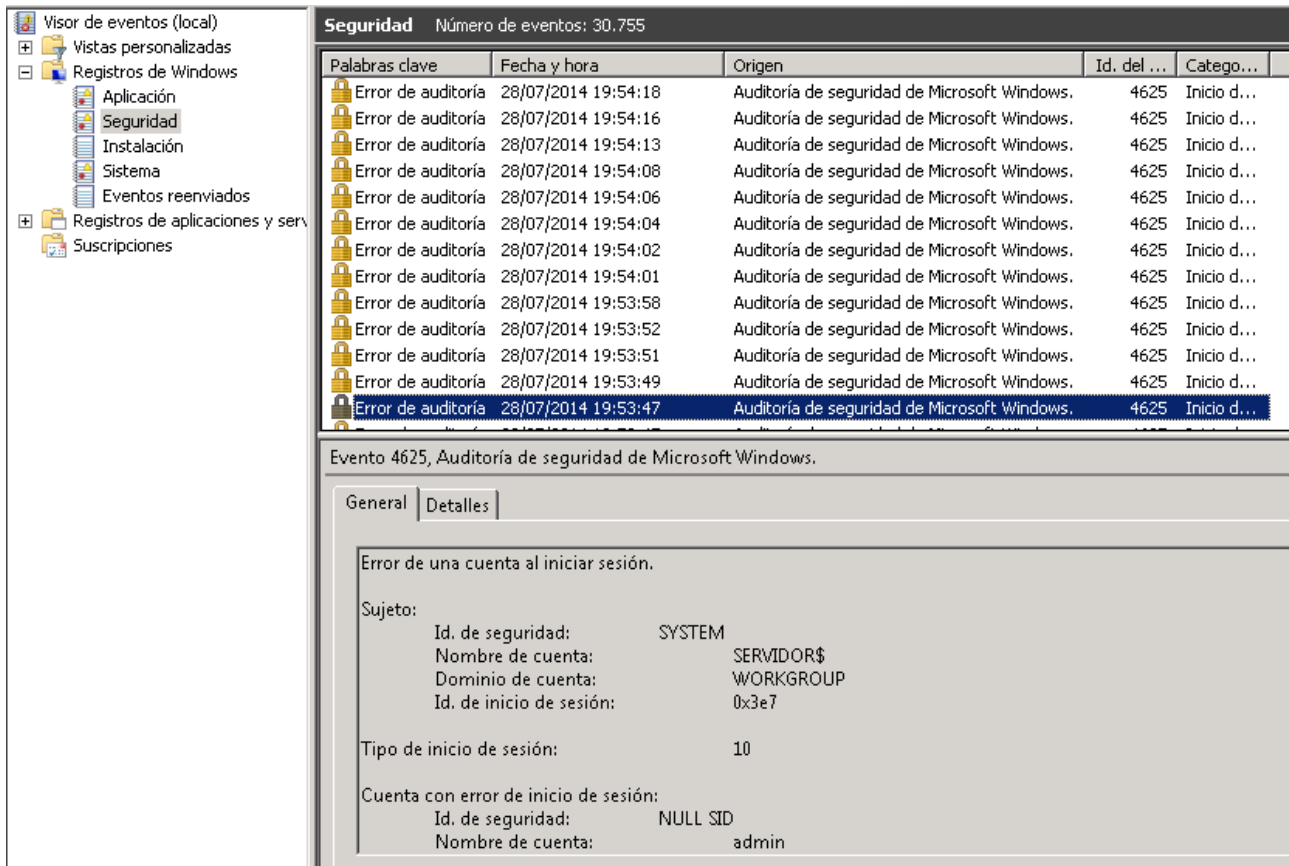
Esto abrirá el visor de sucesos de Windows.

Desde aquí podemos ir en la parte izquierda a “Registro de Windows”, “Seguridad” y podremos ver todos los inicios de sesión que han sido correctos. Son los que tienen como palabras clave “Auditoría Correcta”.



Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	25/08/2014 18:46:12	Microsoft Windows security audi...	4672	Inicio de sesión especial
Auditoría correcta	25/08/2014 18:46:12	Microsoft Windows security audi...	4624	Inicio de sesión
Auditoría correcta	25/08/2014 17:52:36	Microsoft Windows security audi...	4672	Inicio de sesión especial
Auditoría correcta	25/08/2014 17:52:36	Microsoft Windows security audi...	4624	Inicio de sesión
Auditoría correcta	25/08/2014 17:52:31	Microsoft Windows security audi...	4672	Inicio de sesión especial
Auditoría correcta	25/08/2014 17:52:31	Microsoft Windows security audi...	4624	Inicio de sesión
Auditoría correcta	25/08/2014 17:43:59	Microsoft Windows security audi...	4672	Inicio de sesión especial
Auditoría correcta	25/08/2014 17:43:59	Microsoft Windows security audi...	4624	Inicio de sesión

Cuando tenemos intentos de inicio de sesión no válidos entonces la forma que adopta el visor es la siguiente.



Seguridad Número de eventos: 30.755

Palabras clave	Fecha y hora	Origen	Id. del ...	Catego...
Error de auditoría	28/07/2014 19:54:18	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:16	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:13	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:08	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:06	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:04	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:02	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:54:01	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:53:58	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:53:52	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:53:51	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:53:49	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...
Error de auditoría	28/07/2014 19:53:47	Auditoría de seguridad de Microsoft Windows.	4625	Inicio d...

Evento 4625, Auditoría de seguridad de Microsoft Windows.

General Detalles

Error de una cuenta al iniciar sesión.

Sujeto:

Id. de seguridad:	SYSTEM
Nombre de cuenta:	SERVIDOR\$
Dominio de cuenta:	WORKGROUP
Id. de inicio de sesión:	0x3e7

Tipo de inicio de sesión: 10

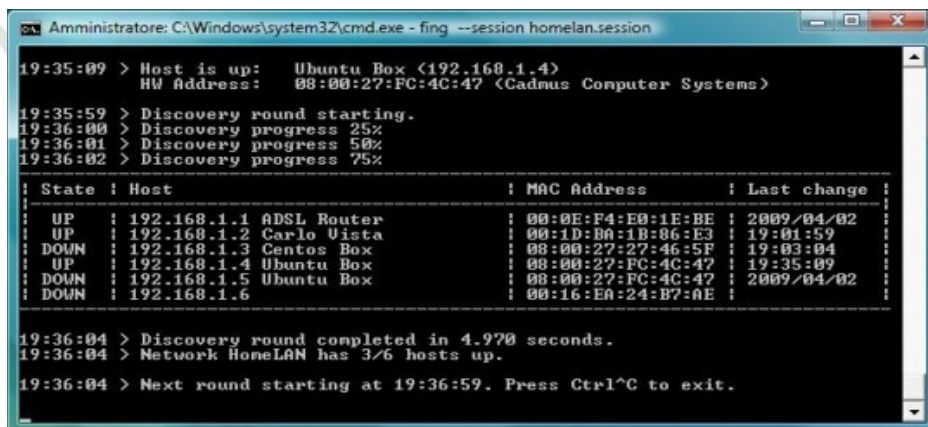
Cuenta con error de inicio de sesión:

Id. de seguridad:	NULL SID
Nombre de cuenta:	admin

Como se puede comprobar existen gran cantidad de Errores de Auditoría en las que podemos ver, entre los detalles, el nombre de la cuenta que se está empleando para el ataque y la IP desde la que se produce.

2º Enumeración de Equipos.

Conocer si tenemos algún equipo en la red es básico para controlar la presencia de ordenadores no deseados. A este proceso se lo conoce como Enumeración de Equipos. Para ello podemos emplear un software específico como Overlook que es gratis.



```

Administrator: C:\Windows\system32\cmd.exe - fing --session homelan.session
19:35:09 > Host is up:  Ubuntu Box (192.168.1.4)
HW Address:  08:00:27:FC:4C:47 (Cadmus Computer Systems)
19:35:59 > Discovery round starting.
19:36:00 > Discovery progress 25%
19:36:01 > Discovery progress 50%
19:36:02 > Discovery progress 75%
-----
| State | Host | MAC Address | Last change |
-----
| UP    | 192.168.1.1 | 00:0E:F4:E0:1E:BE | 2009/04/02 |
| UP    | 192.168.1.2 | 00:1D:8A:1B:86:E3 | 19:01:59 |
| DOWN | 192.168.1.3 | 08:00:27:27:46:5F | 19:03:04 |
| UP    | 192.168.1.4 | 08:00:27:FC:4C:47 | 19:35:09 |
| DOWN | 192.168.1.5 | 08:00:27:FC:4C:47 | 2009/04/02 |
| DOWN | 192.168.1.6 | 08:16:EA:24:B7:AE | |
-----
19:36:04 > Discovery round completed in 4.970 seconds.
19:36:04 > Network HomeLAN has 3/6 hosts up.
19:36:04 > Next round starting at 19:36:59. Press Ctrl+C to exit.
  
```

Con Overlook - Fing podemos realizar diferentes operaciones dentro de nuestra red, como descubrir equipos, asociarlos a una IP, ver qué puertos tiene abiertos esta IP etc.

También cuenta con un modo de centinela que nos alertará si existen intrusos en nuestra red.

Los resultados se pueden mostrar en un formato web html lo que lo hace muy versátil para crear sistemas en línea de mantenimiento y enumeración con Fing.

2014/08/25 19:18:57 overlook fing v2.2

Discovery report of network 192.168.1.0/24 - 2/2 hosts up

< TD>

State	Host	MAC Address	Vendor
UP	192.168.1.1	5C:D9:98:	D-Link
UP	192.168.1.100	70:54:D2:	

2014/08/25 19:18:57 overlook fing