WOOBM HERRAMIENTA PARA AUDITORIA

BY GABRIEL CORONADO

mum
Mikrotik User Meeting

LINE TIME DE LA CONFERENCIA

#mum_bolivia @gabocoronado890

- *Publicando el evento en redes sociales*
- *Presentación del ponente*
- *Conceptualización*
- *Explotación*
- *Conclusiones*

A Cerca del ponente

Jefe de respuesta de incidentes en SSH SUPPORT

- ***Consultor informático Forense.***
- ***Ponente internacional en Argentina, Perú, Paraguay y en varios eventos nacionales.***
- ***Cuento con Varias Certificaciones en ciencia forenses, hacking ético y redes.***
- ***Escritor del libro «»RECUPERACION DE DATOS BASADO EN TECNICAS FORENSE PARA LINUX Y WINDOWS.***
- ***Consultor en varias empresas gubernamentales y privadas***
- ***Partner – elearning para KASPERSKY***

Detalles del libro


kaspersky
Gabriel Coronado Vega
SINIESTRO890
facebook.com/ssh.support
twitter.com/gabocoronado890
ssh.tarija@gmail.com g. coronado@
youtube.com/chanel/UCyUpnuecJAdt7Fc2aYGm76w
70223606

Motivacion de la conferencia

charla de lo que mas nos apasiona

- Conversando con el profesor menciono que era el woobm
- Y después de un rato me lo regalo

Lo convencional

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.41rc28 (c) 1999-2017       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@MikroTik] >
```

#mum_bolivia

@gabocoronado890

Que uso le daremos??

Estamos hablando de siniestro890

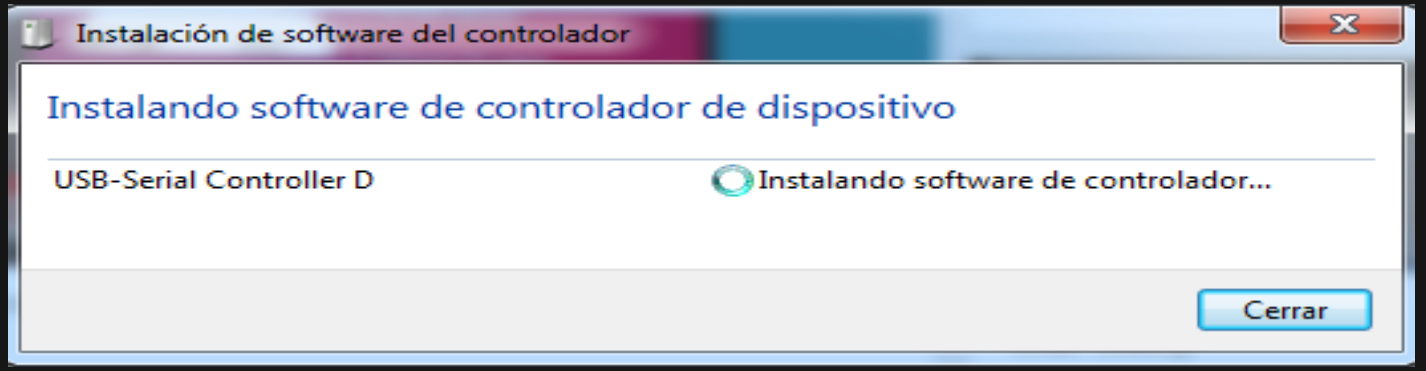
conocen estos juguestes?

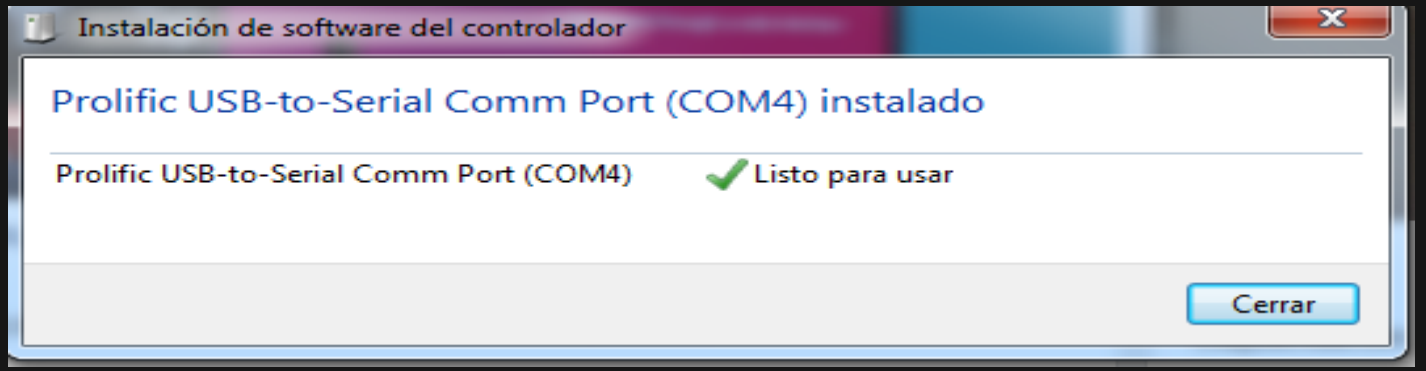
Jefe de respuesta de incidentes en SSH SUPPORT

- ***Consultor informático Forense.***
- ***Ponente internacional en Argentina, Perú, Paraguay y en varios eventos nacionales.***
- ***Cuento con Varias Certificaciones en ciencia forenses, hacking ético y redes.***
- ***Escritor del libro «»RECUPERACION DE DATOS BASADO EN TECNICAS FORENSE PARA LINUX Y WINDOWS.***
- ***Consultor en varias empresas gubernamentales y privadas***
- ***Partner – elearning para KASPERSKY***

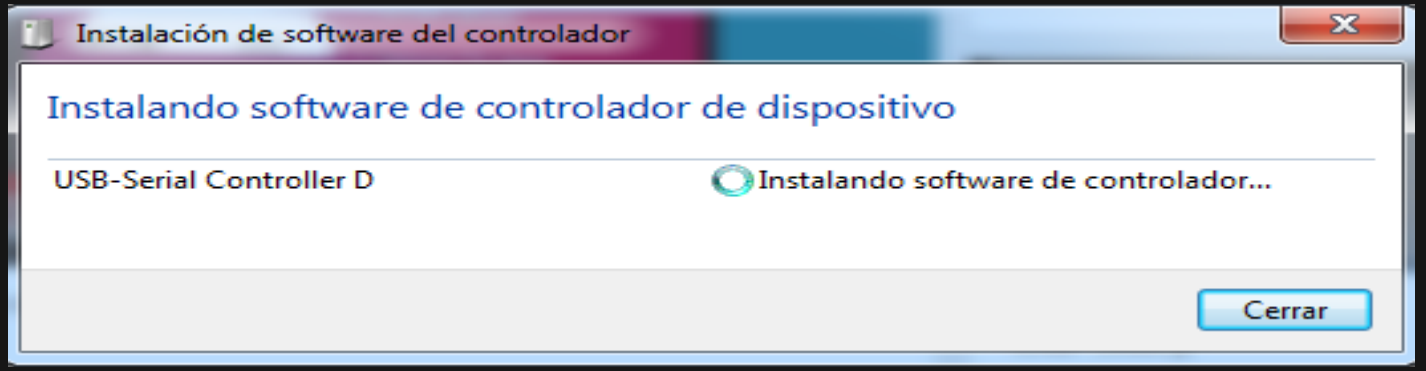
conocen estos juguetes?

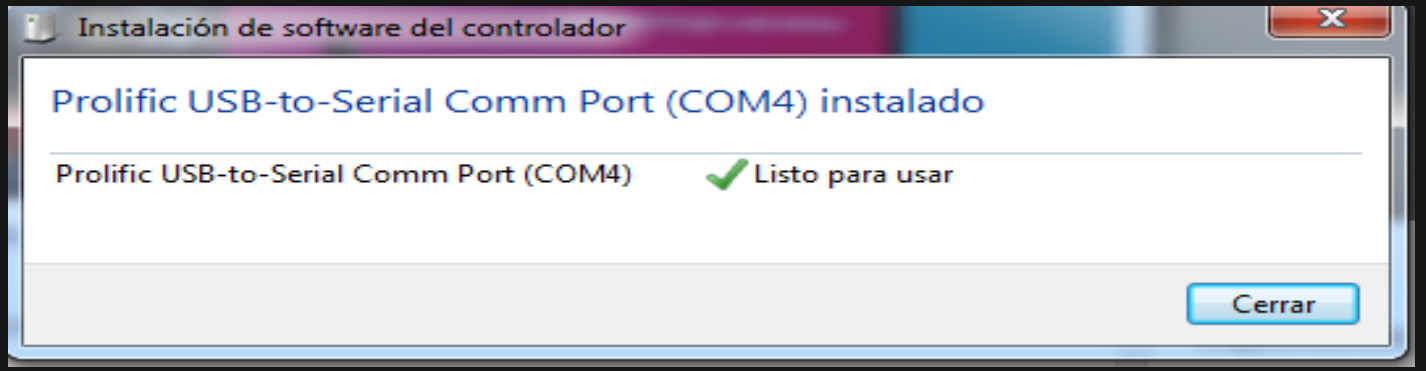
si es usb entonces se puede





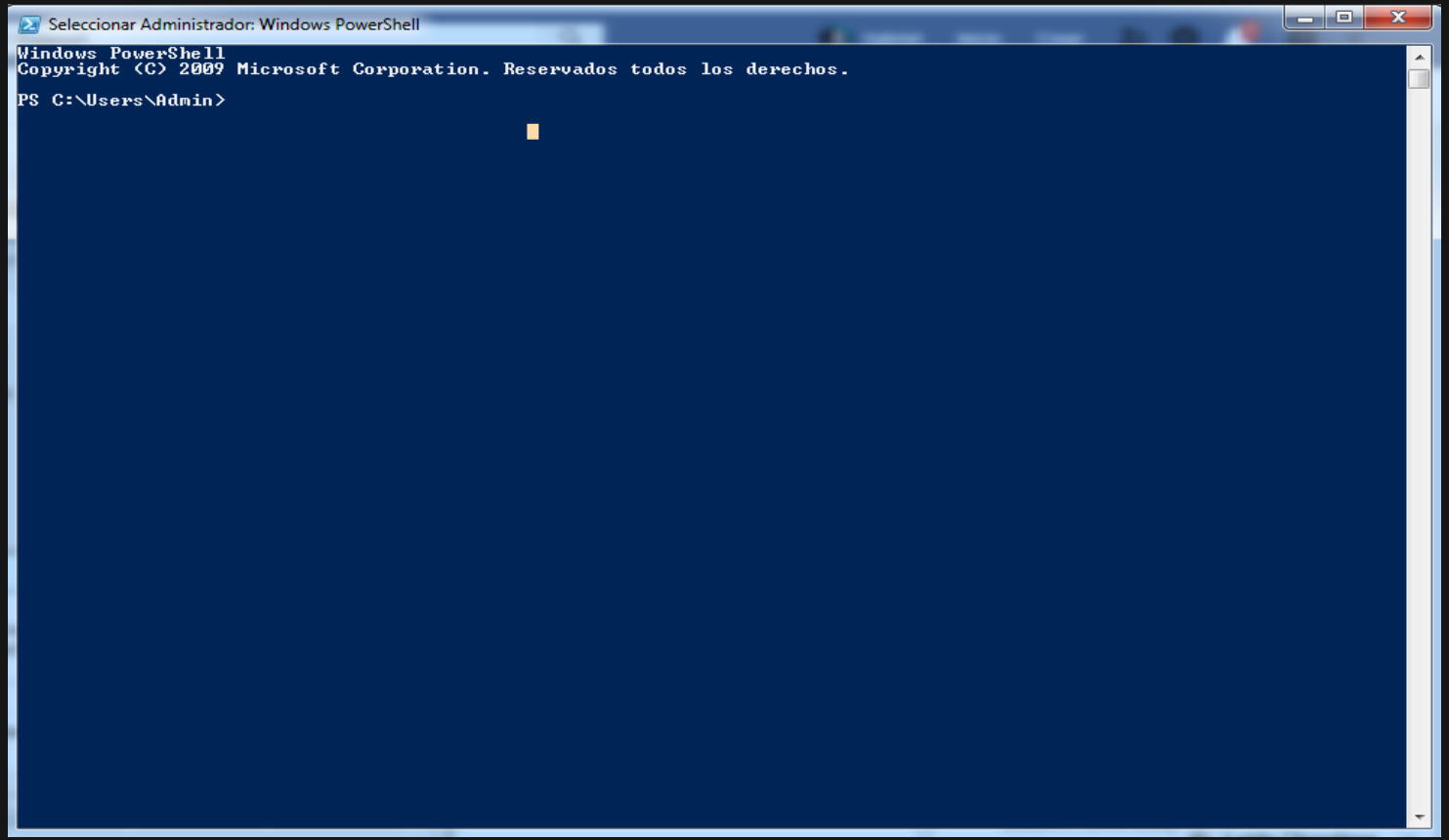
si es usb entonces se puede






kaspersky

jha - jha


Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Reservados todos los derechos.
PS C:\Users\Admin>

jha - jha

aclaración

Preparar un driver especifico para que habrá el powershell

Mi primer librito digital

aura es cuando quien se rinde?

@gabocoronado890 #mum_bolivia

- ***Que mas podemos hacer con el woobm***

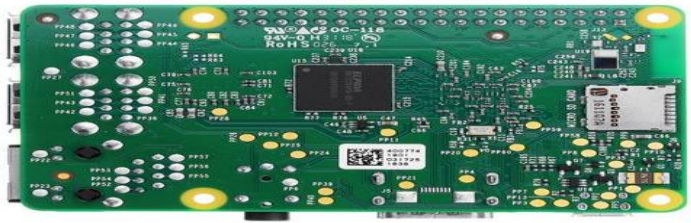
Evil twin una imagen es mejor

Solo el woobm lo hara?


ORA SI
DE CUAL TE FUMASTE CHATO
Imagen creada en GeneradorMemes.com

Necesitamos un herramienta

Objetivo inyectar los paquetes para capturar el password



Usamos un script en phyton

```
echo '0' > /proc/sys/net/ipv4/ip_forward
```

Let's add two function definitions to our utils.py file to provide our script with this functionality:

```
def enable_packet_forwarding():

    with open('/proc/sys/net/ipv4/ip_forward', 'w') as fd:
        fd.write('1')

def disable_packet_forwarding():

    with open('/proc/sys/net/ipv4/ip_forward', 'w') as fd:
        fd.write('0')
```

El resultado de hoy!

172.16.161.1-172.16.161.254

Lista de resultados | Favoritos

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
	172.16.161.98	172.16.161.98	Apple, Inc.	80:82:23:47:D1:4B	
	172.16.161.111	172.16.161.111	HUAWEI TECHNOLOGIE...	24:FB:65:D0:[redacted]	
	172.16.161.116	172.16.161.116		74:4D:28:4B:[redacted]	
	172.16.161.117	172.16.161.117		74:4D:28:5A:[redacted]	
	172.16.161.119	172.16.161.119	Apple, Inc.	38:F9:D3:CA:[redacted]	
	172.16.161.120	172.16.161.120		F4:AF:E7:A6:[redacted]	
	172.16.161.121	172.16.161.121	LG Electronics (Mobile C...	5C:70:A3:7C:[redacted]	
	172.16.161.123	172.16.161.123		F4:AF:E7:A2:[redacted]	
	172.16.161.124	172.16.161.124			
	172.16.161.128	172.16.161.128	Xiaomi Communications...	48:FD:A3:18:[redacted]	
	172.16.161.129	172.16.161.129	SAMSUNG ELECTRO-ME...	08:C5:E1:81:[redacted]	
	172.16.161.130	172.16.161.130	HUAWEI TECHNOLOGIE...	7C:A1:77:2C:[redacted]	
	172.16.161.133	172.16.161.133	Xiaomi Communications...	70:BB:E9:FE:[redacted]	
	172.16.161.136	172.16.161.136			
	172.16.161.139	172.16.161.139	Samsung Electronics Co.,...	FC:A6:21:0D:[redacted]	
	172.16.161.140	172.16.161.140	Murata Manufacturing C...	90:B6:86:48:[redacted]	
	172.16.161.141	172.16.161.141	Apple, Inc.	F4:06:16:C9:[redacted]	
	172.16.161.142	172.16.161.142	Samsung Electronics Co.,...	68:5A:CF:AB:[redacted]	
	172.16.161.143	172.16.161.143	HUAWEI TECHNOLOGIE...	30:A1:FA:55:[redacted]	
	172.16.161.144	172.16.161.144			
	172.16.161.146	172.16.161.146	HUAWEI TECHNOLOGIE...	98:9C:57:56:[redacted]	
	172.16.161.147	172.16.161.147	Xiaomi Communications...	D8:CE:3A:F4:[redacted]	
	172.16.161.148	172.16.161.148	HUAWEI TECHNOLOGIE...	48:3C:0C:9A:[redacted]	
	172.16.161.150	172.16.161.150	Xiaomi Communications...	20:A6:0C:2F:[redacted]	

Agradecido a mis sponsor!

#mum_bolivia

@gabocoronado890

ONE DATA

FUNDACIÓN TECNOLÓGICA EMPRESARIAL CEFIC R.C. 137874

KASPERSKY ANTI-VIRUS

SSH SUPPORT

EcaTel SRL

preguntas?