**Scanning and probing a VPN.**

**by xxradar.**
**http://www.radarhack.com**
**mailto:xxradar@radarhack.com.**

**Version 1.0 16-07-2004**

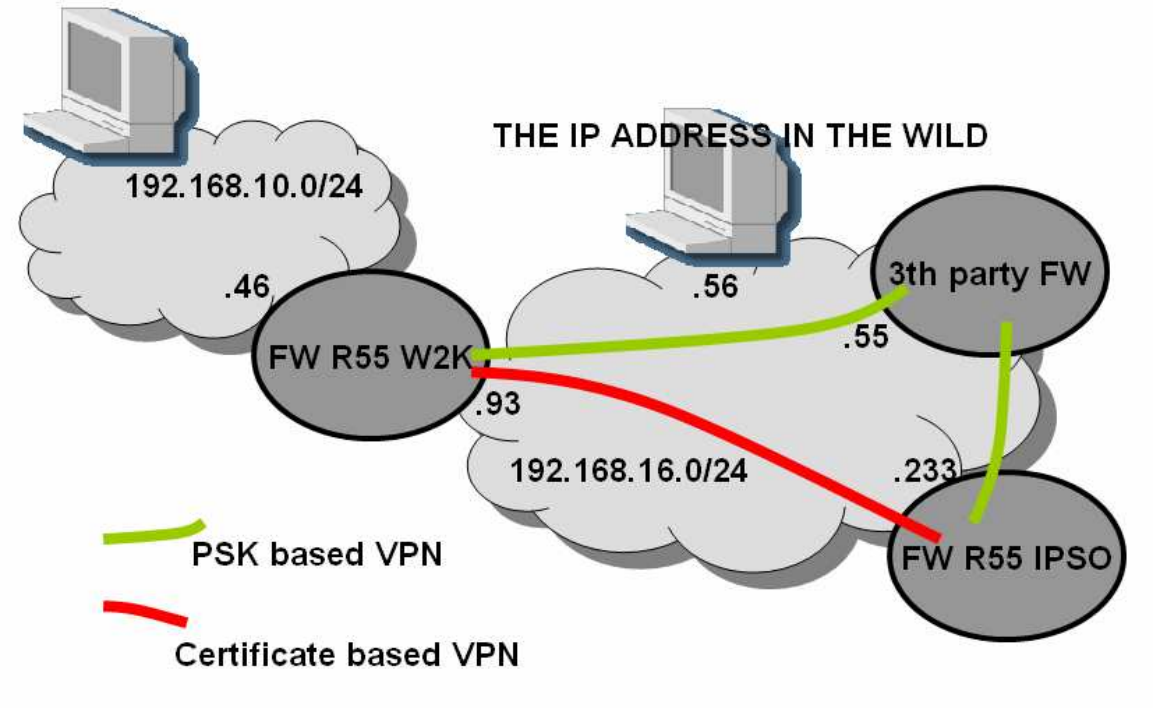
**My summer camp.**

**1. Introduction.**
Wondering on how to use my CPU more intensively during my rainy holidays, I tried to 'mess' a little with some VPN setups. I did not find a lot of info about the topic, but the few useful tools and vulnerabilities I found on the internet made it an interesting experience. This paper simply describes the results of the tests done on a demo VPN.

The tools used are:
*ike-scan.exe* *http://www.nta-monitor.com/ike-scan/*
*ikeprobe.exe* *http://www.ernw.de/download/ikeprobe.zip*

The aim of this paper is not showing how to break a VPN, although it is possible in some scenarios, but showing that VPN's might reveal some info on versions of software, algorithms in use, configuration settings...
The firewalls I used to do the testing (and learning) were a W2K and a NOKIA IP330 running Check Point VPN-1 R55 on W2K and IPSO. My intention is NOT to reveal weaknesses in Check Point and/or NOKIA/W2K software, but analyze what we can get out of the IKE and IPSEC protocols. The tests will show that the default behavior of the firewall is quite restrictive and will reveal little info, although I am aware of vulnerable implementations due to integration with third-party firewall/VPN devices.

The following setup was used to do the testing.
This is a 'simplified meshed site-to-site VPN' with no remote access configured at this point (this is added later in the tests).



**2. Scanning from an IP address in the wild**

This first series of test shows the scanning of the W2K box (with the VPN-1 software installed from an address 'unknown' to the VPN configuration. The use of the tool is straightforward. More info on the 'auth' parameter can be found in the help of the tool, but for this paper:

```
--–auth=1:          Pre-shared key authentication.
--auth=3:           Certificate based authentication.
--auth=64221:       Hybrid mode authentication, used by Remote
                    Access clients to authenticate using SecureID,
                    Radius, tokens…
                    Other codes are available for other vendors.
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
Ending ike-scan 1.6: 1 hosts scanned in 17.482 seconds (0.06 hosts/sec).  0 returned
handshake; 0 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
Ending ike-scan 1.6: 1 hosts scanned in 17.488 seconds (0.06 hosts/sec).  0 returned
handshake; 0 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
Ending ike-scan 1.6: 1 hosts scanned in 17.463 seconds (0.06 hosts/sec).  0 returned
handshake; 0 returned notify
```

The conclusion of this test is that the firewall reveals noting about himself ☺. The firewall only accepts IKE phase 1 negotiations from known devices (configured in the VPN community).
All attempts ARE indeed logged on the system.

**3. Scanning from a trusted and self-managed gateway**

These probes are conducted from the point of view of 'FW R55 IPSO'. Due to this faked IKE negotiation, we can notice that the firewall starts revealing info.

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.113 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=MD5 Auth=RSA_Sig
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
Ending ike-scan 1.6: 1 hosts scanned in 15.050 seconds (0.07 hosts/sec).  1 returned
handshake; 0 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.043 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify
```

Notice that we already can expect a VPN device due to the several ‘0 returned handshake; 1 returned notify’. This reveals already the presences of a VPN enabled device. If we hit the right authentication scheme, the responder ‘acknowledges’ his transformation. (The tool only supports DES version, not AES)

**4. Scanning from an externally managed firewall**

The next probes are conducted from a typical partner site (3rd party FW), which is in most scenarios a pre-shared key VPN.

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=MD5 Auth=PSK
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
Ending ike-scan 1.6: 1 hosts scanned in 15.049 seconds (0.07 hosts/sec).  1 returned
handshake; 0 returned notify
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.046 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.031 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify
```

**5. Trying to determine if Aggressive mode is in use.**

The next series of scans are conducted on FW R55 W2K, once with aggressive mode enable, once with aggressive mode disabled. This modification is often done to make things faster and to increase compatibility with other vendors.

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Aggressive Mode Handshake returned SA=(Enc=3DES Hash=MD5 Auth=PSK
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080) KeyExchange(128
bytes) Nonce(20 bytes) ID(Type=ID_IPV4_ADDR, Value=192.168.10.46) Hash(16 bytes)
Ending ike-scan 1.6: 1 hosts scanned in 15.058 seconds (0.07 hosts/sec).  1 returned
handshake; 0 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.020 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 15.020 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify
```

As you can see, some more info is revealed, even {if you are lucky) the internal IP address of the Firewall.

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 7 (INVALID-EXCHANGE-TYPE)
Ending ike-scan 1.6: 1 hosts scanned in 15.043 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 7 (INVALID-EXCHANGE-TYPE)
Ending ike-scan 1.6: 1 hosts scanned in 15.020 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify

C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 7 (INVALID-EXCHANGE-TYPE)
Ending ike-scan 1.6: 1 hosts scanned in 15.032 seconds (0.07 hosts/sec).  0 returned
handshake; 1 returned notify
```

**6. Running ikeprobe to see if this VPN is vulnerable.**

I added this (to make it fancier ☺), but is only relevant if the VPN is based on:

- aggressive mode
- Pre-shared Key authentication

Please note that this is an IKE problem and not a bug in the firewall software. For more info on the problem, see http://www.ernw.de/download/pskattack.pdf for the theory and an example.

```
C:\tools>ikeprobe 192.168.16.93
IKEProbe 0.1beta   (c) 2003 Michael Thumann (www.ernw.de)
Portions Copyright (c) 2003 Cipherica Labs (www.cipherica.com)
Read license-cipherica.txt for LibIKE License Information
IKE Aggressive Mode PSK Vulnerability Scanner (Bugtraq ID 7423)

Supported Attributes
Ciphers              : DES, 3DES, AES-128, CAST
Hashes               : MD5, SHA1
Diffie Hellman Groups: DH Groups 1,2 and 5

IKE Proposal for Peer: 192.168.16.93
Aggressive Mode activated ...

Attribute Settings:
Cipher DES
Hash SHA1
Diffie Hellman Group 1

  0.000 3: ph1_initiated(00443ee0, 003646f0)
  0.020 3: << ph1 (00443ee0, 244)
  0.030 3: >> 40
  0.030 2: sx_recv_notify: invalid doi
  2.033 3: << ph1 (00443ee0, 244)
  5.037 3: << ph1 (00443ee0, 244)
  8.042 3: ph1_disposed(00443ee0)
...
Attribute Settings:
Cipher 3DES
Hash MD5
Diffie Hellman Group 1

 72.004 3: ph1_initiated(00443ee0, 00364b98)
 72.034 3: << ph1 (00443ee0, 244)
 72.044 3: >> 40
 72.044 2: sx_recv_notify: invalid doi
 74.047 3: << ph1 (00443ee0, 244)
 77.051 3: << ph1 (00443ee0, 244)
 80.055 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash MD5
Diffie Hellman Group 2

 80.055 3: ph1_initiated(00443ee0, 003646f0)
 80.125 3: << ph1 (00443ee0, 276)
 80.145 3: >> 260
 80.216 3: ph1_get_psk(00443ee0)

*************************************************************************
* System is vulnerable!! See http://www.securityfocus/bid/7423/ for details *
*************************************************************************
```

**7. Trying to fingerprint the firewall when remote access is enabled.**
Up to now, the scanning is only relevant if we are sitting on 'legitimate' IP addresses. Let's turn on Remote Access, and see what we get out of the setup.
The firewall is configured with a user, allowed to login with a certificate and a One-Time password device (hybrid mode). (We can use pre-shared key authentication with users, but is this unmanageable en disabled by default). For this, I created a Remote Access Community on the firewall. At this moment, all tests are conducted from a 'hackers' perspective, an IP address in the wild.

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=1
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 14 (NO-PROPOSAL-CHOSEN)
Ending ike-scan 1.6: 1 hosts scanned in 0.068 seconds (14.71 hosts/sec).  0 returned
handshake; 1 returned notify
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=SHA1 Auth=RSA_Sig
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
Ending ike-scan 1.6: 1 hosts scanned in 1.069 seconds (0.94 hosts/sec).  1 returned
handshake; 0 returned notify
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=SHA1 Auth=64221
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
Ending ike-scan 1.6: 1 hosts scanned in 0.038 seconds (26.32 hosts/sec).  1 returned
handshake; 0 returned notify
```

Ike-scan can be used to scan a range of IP addresses, so scanning for –-auth=64221, might reveal Remote Access devices (remember, different parameters are necessary for other vendors)

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=3 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 29 (UNSUPPORTED-EXCHANGE-TYPE)
Ending ike-scan 1.6: 1 hosts scanned in 0.031 seconds (32.26 hosts/sec).  0 returned
handshake; 1 returned notify
```

```
C:\tools\ikescan>ike-scan 192.168.16.93 --auth=64221 -A
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.16.93   Notify message 29 (UNSUPPORTED-EXCHANGE-TYPE)
Ending ike-scan 1.6: 1 hosts scanned in 0.039 seconds (25.64 hosts/sec).  0 returned
handshake; 1 returned notify
```

Notice that remote access does not support aggressive mode (and I did not manage to turn it on in simplified VPN configurations (but this could be due to myself), so we do not suffer (certainly by default) from the possible pre-shared key attack described earlier.

**8. Fingerprinting via the IKE backup algorithm**

The next scan tries to 'fingerprint' the type of firewall by analyzing the ike-backoff algoritm. Thise might render the type of firewall in use.

```
C:\tools\ikescan>ike-scan --showbackoff -v -v 192.168.16.93   --auth=3
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
---     Sending packet #1 to host entry 1 (192.168.16.93) tmo 500000 us
---     Received packet #1 from 192.168.16.93
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=SHA1 Auth=RSA_Sig
 Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
---     Removing host entry 1 (192.168.16.93) - Received 84 bytes
---     Received packet #2 from 192.168.16.93
---     Received packet #3 from 192.168.16.93
---     Received packet #4 from 192.168.16.93
---     Received packet #5 from 192.168.16.93
---     Received packet #6 from 192.168.16.93
---     Received packet #7 from 192.168.16.93
---     Received packet #8 from 192.168.16.93
---     Received packet #9 from 192.168.16.93
---     Received packet #10 from 192.168.16.93
---     Received packet #11 from 192.168.16.93
---     Received packet #12 from 192.168.16.93

IKE Backoff Patterns:

IP Address      No.     Recv time               Delta Time
192.168.16.93   1       1089918188.002712       0.000000
192.168.16.93   2       1089918189.996712       1.994000
192.168.16.93   3       1089918191.998712       2.002000
192.168.16.93   4       1089918194.001712       2.003000
192.168.16.93   5       1089918196.003712       2.002000
192.168.16.93   6       1089918198.005712       2.002000
192.168.16.93   7       1089918200.008712       2.003000
192.168.16.93   8       1089918204.014712       4.006000
192.168.16.93   9       1089918208.018712       4.004000
192.168.16.93   10      1089918212.023712       4.005000
192.168.16.93   11      1089918216.028712       4.005000
192.168.16.93   12      1089918220.033712       4.005000
192.168.16.93   Implementation guess: Firewall-1 4.1/NG

Ending ike-scan 1.6: 1 hosts scanned in 92.258 seconds (0.01 hosts/sec).  1 retu
rned handshake; 0 returned notify

C:\tools\ikescan>
```

**9. Fingerprinting via the VENDOR ID**

A more accurate way of fingerprinting is by supplying a VENDOR ID. The –-vendor=xxxx supplied is from an earlier version of the software, but as you can see, the firewall responds with his version of the software. This test can only be done if you are using an IP address known in the site-to-site configuration and NOT from a remote access location.

```
C:\tools\ikescan>ike-scan -v -v 192.168.16.93   --auth=3
--vendor=f4ed19e0c114eb
516faaac0ee37daf2807b4381f0000000100001389000000000000000000....0000
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
---     Sending packet #1 to host entry 1 (192.168.16.93) tmo 500000 us
---     Received packet #1 from 192.168.16.93
192.168.16.93   Main Mode Handshake returned SA=(Enc=3DES Hash=MD5 Auth=RSA_Sig
Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080) VID=f4ed19e0c114eb
516faaac0ee37daf2807b4381f000000010000138d000000000000000018000000 (Firewall-1 N
G AI R55)
---     Removing host entry 1 (192.168.16.93) - Received 128 bytes

Ending ike-scan 1.6: 1 hosts scanned in 1.096 seconds (0.91 hosts/sec).  1 returned
handshake; 0 returned notify
```

**10. Conclusion**

I concluded from this test that the default configuration of my test environment revealed not so much information, if you do NOT have access from an ‘authorized’ IP address.

I would on the other hand advice NOT to use the aggressive mode feature if possible, since I can think of scenarios (with HIDE NAT and VPN configured on the same box) where this might lead to problems. Please consider that these tests are not complete and may contain errors. If you have questions or remarks, please let me know.