M2RIP
Sécurité Avancée des réseaux

IKE-scan

Besma CHAOUCH

2011-2012

Introduction

- discovering
- fingerprinting
- testing

} IP sec VPN systems

VPN , **V**irtual **P**rivate **N**etwork

(+) coût moins cher (pas d'infrastructure particulière, exploite le réseau Internet)

Objectif : Sécuriser les communications entre 2 entités distantes (notion de Tunnel) traversant une zone n'appartenant pas en exclusivité à ces deux entités communicantes

Principe : Dédier un « VP » (virtual path) à un VPN

Authentification des extrémités communicantes & Chiffrage des données par le biais du protocole IPsec

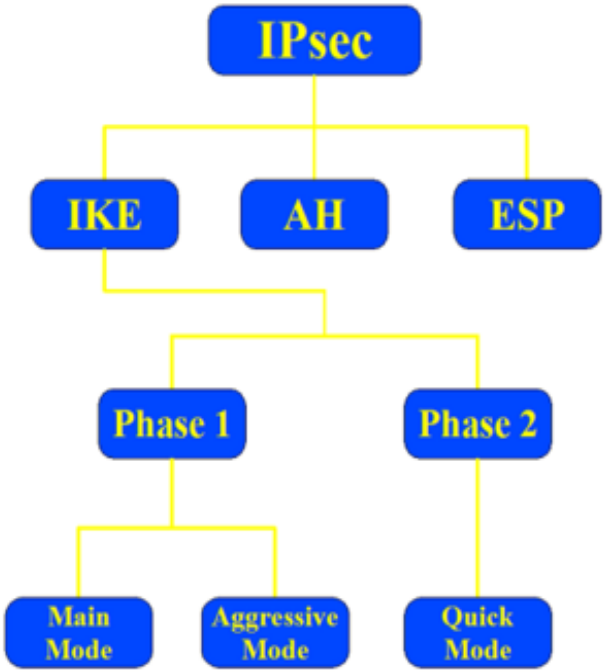
IPsec : encapsulation des paquets IP + cryptage

IKE-scan

Il génère et envoie des paquets IKE Phase-1 aux hôtes spécifiés, et affiche toutes les réponses qui sont reçues.

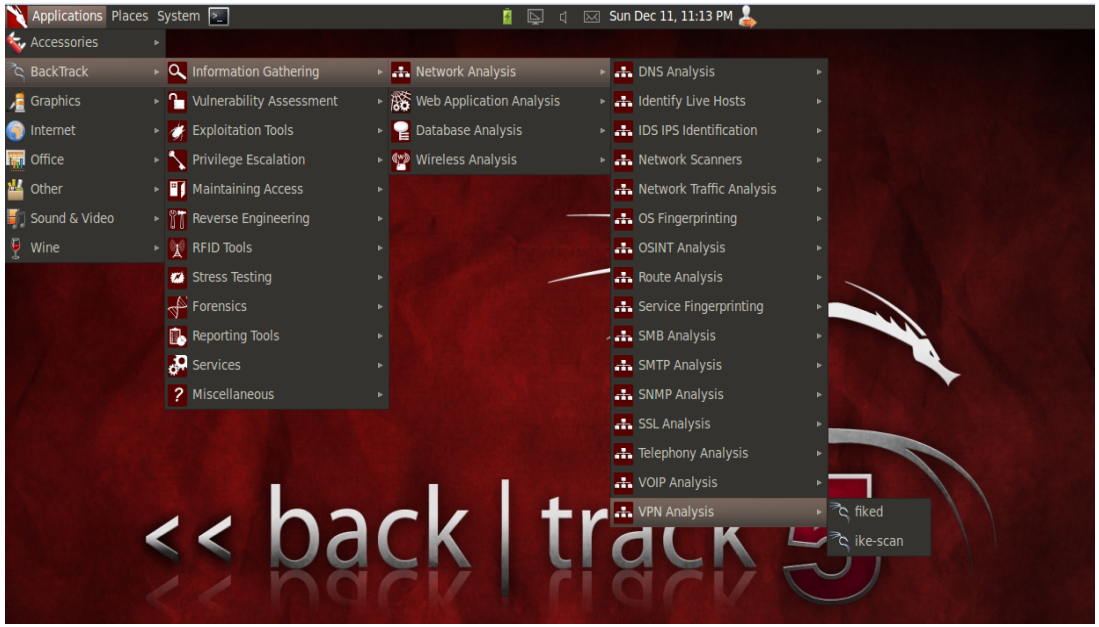
IKE , Internet **K**ey **E**xchange

* Sous protocole de l'IPsec,
* Mise en place d'un mécanisme d'authentification et d'échange des clés utilisé par le protocole IPsec.



IKE-scan sous BackTrack

menu Application : Backtrack | Information Gathering |Network Analysis|VPN Analysis|Ike-scan



Ike-scan

IKE-scan sous BackTrack

- scan à partir d'une @ IP
- Plusieurs options à manipuler

```
root@bt:~# ike-scan -M 192.168.0.98
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

Ending ike-scan 1.9: 1 hosts scanned in 2.499 seconds (0.40 hosts/sec).  0 retur
ned handshake; 0 returned notify
root@bt:~# ike-scan -M -v 192.168.0.98
DEBUG: pkt len=336 bytes, bandwidth=56000 bps, int=52000 us
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
---     Pass 1 of 3 completed
---     Pass 2 of 3 completed
---     Pass 3 of 3 completed

Ending ike-scan 1.9: 1 hosts scanned in 2.491 seconds (0.40 hosts/sec).  0 retur
ned handshake; 0 returned notify
```

=> Le serveur ne révèle rien sur lui-même, accept uniquement les négociations IKE-phase1 depuis des machines connues (appartenant au VPN en question)

IKE-scan sous BackTrack

ike-scan -M -v 192.168.109.99

```
DEBUG: pkt len=336 bytes, bandwidth=56000 bps, int=52000 us
Starting ike-scan 1.9 with 32 hosts (http://www.nta-monitor.com/tools/
ike-scan/)
192.168.109.99   Main Mode Handshake returned HDR=(CKY-
R=4c6950d4ff3bede2) SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024
LifeType=Seconds LifeDuration=28800) VID=afcad71368a1f1c96b8696
fc77570100 (Dead Peer Detection v1.0)
```

Les informations les plus importantes est dans le champ **SA** :

Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration=28800

Triple-DES pour le cryptage ,

SHA1 comme algorithme d'hachage ,

Pre-Shared Key (PSK): méthode d'authentification,

Diffie-Hellman group 2 (pour l'échange des clés de chiffrement, clés à 1024 bits),

Et le SA lifetime (temps de vie) est de 28800 seconds.

Fingerprinting

Fingerprinting via the IKE backup Algorithm

```
$ ike-scan -M --trans=5,2,1,2 --showbackoff 10.0.0.1
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
10.0.0.1      Main Mode Handshake returned
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)

IKE Backoff Patterns:

IP Address      No.     Recv time               Delta Time
10.0.0.1        1       1121251508.773117       0.000000
10.0.0.1        2       1121251510.772474       1.999357
10.0.0.1        3       1121251512.775259       2.002785
10.0.0.1        4       1121251514.777952       2.002693
10.0.0.1        5       1121251516.780746       2.002794
10.0.0.1        6       1121251518.783504       2.002758
10.0.0.1        7       1121251520.786298       2.002794
10.0.0.1        8       1121251524.791781       4.005483
10.0.0.1        9       1121251528.797329       4.005548
10.0.0.1        10      1121251532.802822       4.005493
10.0.0.1        11      1121251536.808370       4.005548
10.0.0.1        12      1121251540.813874       4.005504
10.0.0.1        Implementation guess: Firewall-1 4.1/NG/NGX
```

```
$ ike-scan -M --trans=5,1,1,2 --showbackoff 10.0.0.2
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
10.0.0.2 Main Mode Handshake returned
        SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

IKE Backoff Patterns:

IP Address      No.     Recv time               Delta Time
10.0.0.2        1       1121252105.954742       0.000000
10.0.0.2        2       1121252113.946698       7.991956
10.0.0.2        3       1121252121.944037       7.997339
10.0.0.2        4       1121252129.945608       8.001571
10.0.0.2        Implementation guess: Cisco VPN Concentrator
```

Fingerprinting

Fingerprinting via the vendor ID

```
$ ike-scan --trans=5,2,1,2 --vendor=00 --multiline 10.0.0.3
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
10.0.0.3     Main Mode Handshake returned
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
        VID=424e455300000009 (Nortel Contivity)
```

IKE-scan en mode aggressif

Le mode agressif: (Aggressive Mode)

- mode optionnel de l'IKE phase1
- beaucoup plus simple que le mode principal (Main Mode)
- (-) moins flexible que « MM » , permet plusieurs failles de sécurité.

=> authentification par les clés pré-partagées (PSK, Pre-shared key authentification)

- pour les solutions d'accès distant (remote Access)

```
$ ike-scan --aggressive --multiline --id=finance_group 10.0.0.2
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
10.0.0.2 Aggressive Mode Handshake returned
        SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        KeyExchange(128 bytes)
        Nonce(20 bytes)
        ID(Type=ID_IPV4_ADDR, Value=10.0.0.2)
        Hash(16 bytes)
        VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
        VID=09002689dfd6b712 (XAUTH)
        VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
        VID=1f07f70eaa6514d3b0fa96542a500306 (Cisco VPN Concentrator)
```

Merci de votre attention