Licence SEICOM
Module M37
«Sécurité – Tests d'intrusion »

Philippe Mercier
Pierrick Tasse

5 – Sécurité – Tests d'intrusion

Cartographie réseau à distance
La collecte d'informations
Nmap
Scapy
Outils de protection : NIDS
Outils de protection : Nessus
Les failles logicielles : 0Day
Outils de tests de pénétration : Metasploit

Cartographie réseau à distance (1)

- Avant d'entreprendre un test d'intrusion, il est nécessaire de récolter des informations sur les ressources à tester (attaquer).
- Les 3 phases pour cartographier un réseau cible :
  - Délimiter le périmètre de l'infrastructure cible (noms de domaine, @IP, répartition géographique, FAI, ...)
    - whois
  - Découverte des services accessibles.
    - rpcinfo, nmap
  - Découverte du réseau en profondeur (routeurs, pare-feu, services par machine, etc.).
    - traceroute, scapy

La collecte d'informations

- Les outils utilisés par les pirates pour attaquer un système sont très utiles pour ...
- ... se protéger de ces attaques
- La référence : **nmap**

- Un scanner est un outil logiciel qui interroge un serveur afin d'identifier les services en attente de connexion.
- Un service est associé à un port (TCP/UDP).

nmap (1)

- **nmap** : scanner utilisé pour tester la sécurité d'une machine ou d'un réseau.
- **nmap** permet de découvrir les informations suivantes sur un réseau :
  - Machines connectées
  - Ports ouverts, fermés et filtrés
  - Système d'exploitation et application
- Syntaxe de la commande :

```
nmap [type de scan] [options] <machine ou réseau>
```

- zenmap : interface graphique de nmap (ou mapfe).

nmap (2)

- Exemple : scanner les services locaux

```
# nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-02
17:15 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
631/tcp  open  ipp
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.06
seconds
```


nmap (3)

- Plusieurs de types de scan TCP :
  - connect scan (-sT) : connexion effective sur chaque port scanné
  - syn scan (-sS) : émission SYN, attente ACK + RST (+ furtif)
- Exemple : scan de ports TCP avec sauvegarde

```
# nmap -p 1-65535 -T4 -A -v 10.10.10.0/24
# nmap -sS -P0 -A -oA scan-result -p 1-65535 10.10.10.0/24
```

  - Sélection de tous les ports (-p 1-65535)
  - Sélection de toutes les machines du sous-réseau (/24)
  - Détection du type d'OS et service (-A)
  - Le tout même si la machine ne répond pas au ping (-P0)
  - Sauvegarde des résultats dans des formats XML et texte simple

nmap (4)

- Exemple : extrait du résultat du scan précédent

```
Interesting ports on 10.10.10.15:
Not shown: 65530 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 4.3p2 Debian 9 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.2.3 ((Debian) PHP/5.2.0-8+etch7)
111/tcp  open  rpc
113/tcp  open  ident   OpenBSD identd
3540/tcp open  status   1 (rpc #100024)
MAC Address: 00:10:D7:09:6C:79 (Argosy Research)
No exact OS matches for host (If you know what OS is running on it,
see http://insecure.org/nmap/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=4.20%D=12/8%OT=22%CT=1%CU=40308%PV=Y%DS=1%G=Y
%M=0010D7%TM=475AD5B
...

Uptime: 0.084 days (since Sat Dec  8 16:33:18 2007)
Network Distance: 1 hop
Service Info: OSs: Linux, OpenBSD
```

Nmap (5)

- Exemple : découverte de machines sur un réseau

```
# nmap -sP 10.10.10.0/24
Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-10 21:47
CET
Host 10.10.10.1 appears to be up.
MAC Address: 00:14:69:78:BB:BA (Cisco Systems)
Host 10.10.10.2 appears to be up.
MAC Address: 00:1A:4B:0E:26:62 (Unknown)
Host 10.10.10.13 appears to be up.
Host 10.10.10.14 appears to be up.
MAC Address: 00:D0:E0:90:8E:C0 (Dooin Electronics CO.)
Host 10.10.10.15 appears to be up.
MAC Address: 00:10:D7:09:6C:79 (Argosy Research)
Host 10.10.10.200 appears to be up.
MAC Address: 00:04:76:A3:31:16 (3 Com)
Nmap finished: 256 IP addresses (6 hosts up) scanned in 4.932
seconds
```

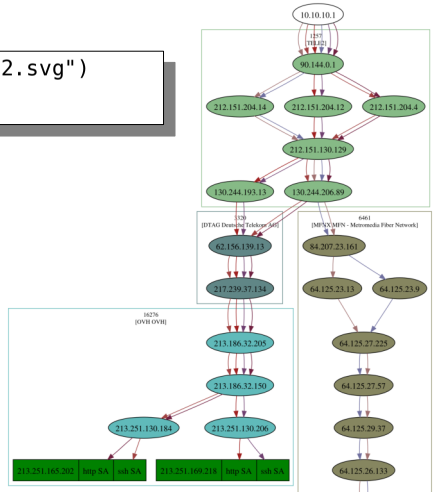

Scapy (1)

- **Scapy** est un programme de manipulation de paquets pour le scanning, tracerouting, sondage réseau, test ou attaque d'équipement, découverte de réseau, injection de paquets 802.11, arp cache poisoning, décodage VOIP sur canal encrypté avec WEP, ...
- Scapy améliore l'interprétation des résultats avec des affichages graphiques (2D ou 3D)

```
Welcome to Scapy (2.2.0)
>>> res,unans =
traceroute(["ns34189.ovh.net","ns33257.ovh.net","pedagogie.ac-
nantes.fr"],dport=[80,22],maxttl=20,retry=-2)
Begin emission:
************************************************************
**************************************Finished to send 120
packets....
```

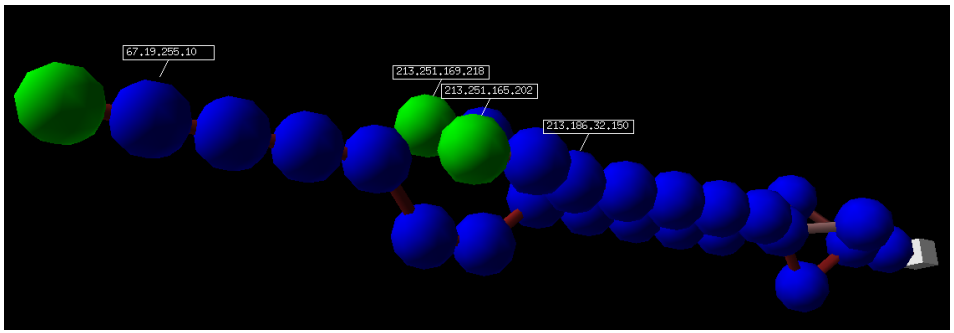

Scapy (2)

```
>>> res.graph(target="> /tmp/graph2.svg")
```



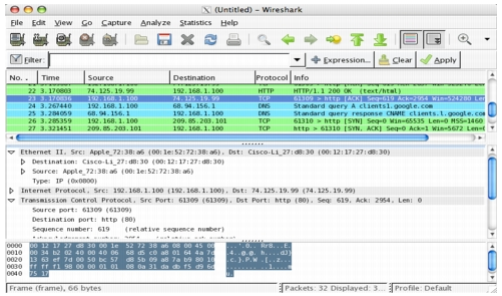
Scapy (3)

```
>>> res.trace3D()
```

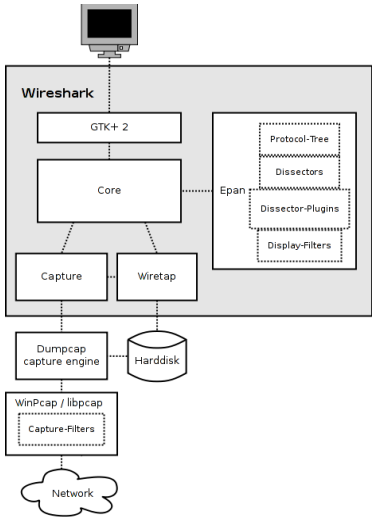


Outil d'analyse : wireshark (1)

- Sécurité préventive : comment se comporte un nouveau logiciel ? Respect CdC, RFC ? Données émises/reçues ?
- Sécurité réactive/défensive : analyse trafic attaque
- Résolution d'incidents : debugger réseau



Outil d'analyse : wireshark (2)



Outil d'analyse : wireshark (3)

- tshark
- Filtrage pré/post capture : filtrer le moins possible avant la capture.
- Vulnérabilité de wireshark :
  - Droit admin sur les cartes réseau
  - Failles de sécurité dans les dissecteurs...

```
$ sudo dumpcat -i eth0 -w - | wireshark -k -i -
```


Outil d'analyse : wireshark (4)

- Informations à extraire de la capture à l'aide des outils de statistique :
  - Liste des adresses IP sources / destinations
  - Liste des protocoles utilisés
  - Volumétrie des données échangées
  - Erreurs contenues dans le trafic :
    - Paquets perdus ou dupliqués
    - Message d'erreur ICMP
    - Paquet mal formés et anormaux
- Cartographie des conversations : qui parle avec qui ?
- Isoler les machines suspectes (volumes ou protocoles anormaux)

Outils de protection : les systèmes de détection d'intrusion

- NIDS : Network Intrusion Detection System
- Ces utilitaires inspectent le trafic du réseau afin de détecter les attaques en temps réel. Ils contiennent une base de données des codes malicieux et peuvent détecter leur passage sur le réseau.
- Les plus connus :
  - Prelude Hybrid IDS
  - Snort : sniffer, packet logger et NIDS

Outils de protection : les systèmes de détection d'intrusion

```
# snort -i eth0 -A console -c /etc/snort/snort.conf
Running in IDS mode
--== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.3.3 (Build 14)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           (C) Copyright 1998-2004 Sourcefire Inc., et al.

03/04-13:11:14.287978  [**] [122:17:0] (portscan) UDP Portscan [**]
        {RAW} 213.251.169.218 -> 213.251.169.251
03/04-13:11:18.026399  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
        [Classification: Detection of a Network Scan] [Priority: 3]
        {UDP} 213.251.169.182:1900 -> 239.255.255.250:1900
03/04-13:11:33.207235  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
        [Classification: Detection of a Network Scan] [Priority: 3]
        {UDP} 213.251.169.168:8008 -> 239.255.255.250:1900
```

Exemple de règle :

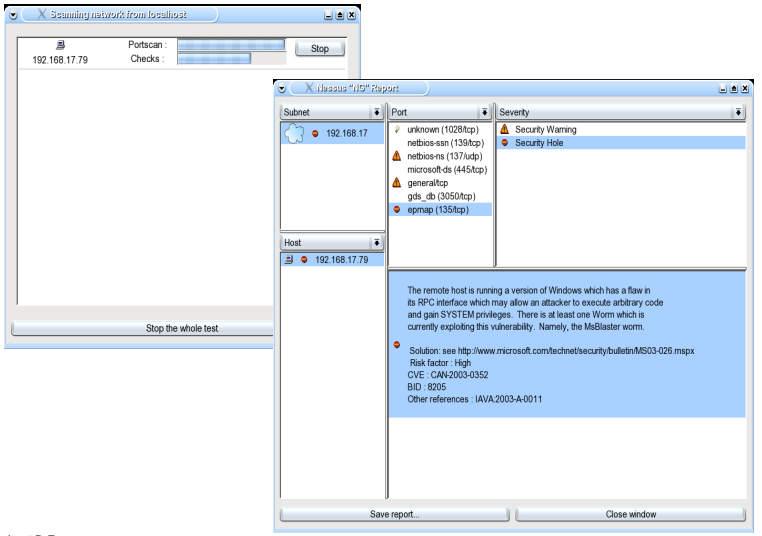
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)

Outils de protection : Nessus (1)

- Outil de sécurité permettant de scanner une ou plusieurs machines.
- Permet de tester différentes attaques pour savoir si des machines sont vulnérables.
- Logiciel client/serveur
  - Serveur : base de données et moteur des tests
  - Client : configuration, lancement et exploitation des tests

- Note : Nessus étant devenu payant sur sa version illimitée, un fork appelé OpenVAS existe sous linux avec les mêmes fonctionnalités.

Outils de protection : Nessus (2)



Les failles logicielles : Vocabulaire

- **POC** (Proof Of Concept) : programme démontrant la faisabilité d'une attaque exploitant une faille informatique
- **Exploit** : programme utilisé pour profiter d'une faille dans un logiciel (système d'exploitation ou application) pour prendre le contrôle d'un ordinateur et de ses données.
- **Payload** (ou charge virale) : code malicieux que chacun ajoutera au POC en fonction de ses besoins
- **Faille 0 day** : trou de sécurité informatique gardé confidentiel, ou connu par un nombre très restreint de personnes, ainsi que la manière de l'exploiter (via un logiciel malveillant nommé exploit)

http://www.lemonde.fr/pixels/article/2015/09/23/le-business-des-zero-day-ces-failles-inconnues-des-fabricants-de-logiciel_4768638_4408996.html

Les failles logicielles : Définition du 0day

- Phase 1: Pre-Discovery – The vulnerability exists, but no one has identified it.
- Phase 2: Discovery – The vulnerability is identified, but not yet announced.
- Phase 3: Announcement – The vulnerability is publicly announced, making users and attackers alike aware of the vulnerability.
- Phase 4: Exploit – An automated code is published that exploits the vulnerability.
- Phase 5: Patch – A software patch is issued to close the vulnerability

Les failles logicielles : exemples

- vmsplice

Tuesday, February 19, 2008

SARA Linux Malware

Hi all!
I released today a basic malware for to exploit the vmsplice bug on Linux kernel.
This program use the vulnerability for install some backdoors on system.

UPDATED
Actions:
- disable INPUT rules on firewall
- open the 1407 port for execute remote commands
- open a bash session on 14071 port using the xinetd daemon
- add a admin user without password
- schedule malicious tasks on cron
- mail the shadow file for a mail account

Vulnerables systems: Linux 2.6.17 - 2.6.24.1

Warning:
THIS IS A MALWARE. DON'T RUN IT IF YOU DON'T KNOW WHAT YOU ARE DOING.

Download:
http://coarseknocking.sourceforge.net/sara/sara-malware-0.0.2.tar.gz
Posted by si0ux at 6:39 AM

Les failles logicielles : exemples

- ssh...

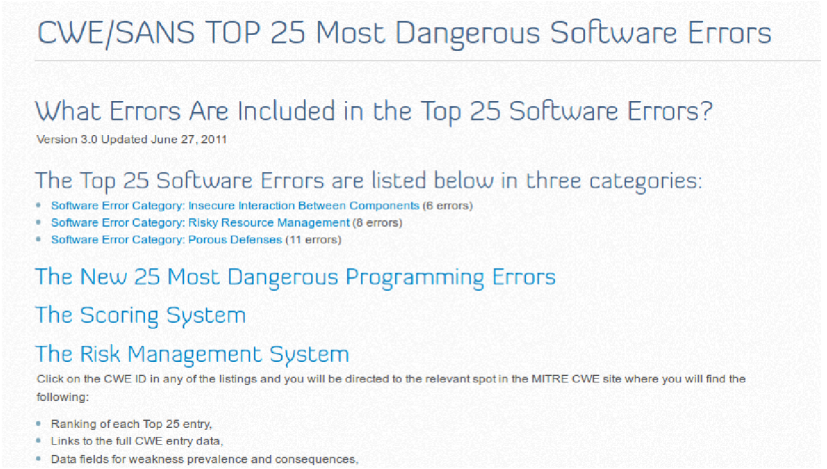
```
Sujet : Debian generated SSH-Keys working exploit
De :  mm@deadbeef.de
À : bugtraq@securityfocus.com
Date : 2008-05-15 07:5

Hi Securityfocus,

the debian openssl issue leads that there are only 65.536 possible
ssh keys generated, cause the only entropy is the pid of the process
generating the key.

This leads to that the following perl script can be used with the
precalculated ssh keys to brute force the ssh login. It works if such
a keys is installed on a non-patched debian or any other system manual
configured to.

On an unpatched system, which doesn't need to be debian, do the following:

1. Download http://www.deadbeef.de/rsa.2048.tar.bzip2
...
```

Outils de tests de pénétration : Metasploit

- Metasploit est une plate-forme de référence dans le monde de l'audit de sécurité.
- Cet outil permet de faire (entre autre) des tests de pénétration dans un réseau en exploitant des failles logicielles présentes sur des équipements de ce réseau.
- http://www.metasploit.com
- https://www.exploit-db.com/

TOP 25 Most Dangerous Programming Errors

- http://www.sans.org/top25errors/


CWE/SANS TOP 25 Most Dangerous Software Errors

What Errors Are Included in the Top 25 Software Errors?

Version 3.0 Updated June 27, 2011

The Top 25 Software Errors are listed below in three categories:

- Software Error Category: Insecure Interaction Between Components (6 errors)
- Software Error Category: Risky Resource Management (8 errors)
- Software Error Category: Porous Defenses (11 errors)

The New 25 Most Dangerous Programming Errors

The Scoring System

The Risk Management System

Click on the CWE ID in any of the listings and you will be directed to the relevant spot in the MITRE CWE site where you will find the following:

- Ranking of each Top 25 entry,
- Links to the full CWE entry data,
- Data fields for weakness prevalence and consequences,

Présentation du TP final

- Mise en place de l'infrastructure
  - Mise en place de l'infrastructure "ouverte" aux attaques
  - Sécurisation de l'infrastructure
- Attaques
- Échange des infrastructures
  - audit de sécurité de la configuration adverse
- Présentations de chaque équipe (avec diaporama)