
<<back|track
@OSSIR France

Giovanni RATTARO

Renaud LEROY

Consultants Sécurité

OpenMinded-Consulting

"The quieter you become, the more you are able to hear."

<< back | track 5

SOMMAIRE

- Sécurité Informatique Classique VS Sécurité Informatique proactive
- Nécessité d'une nouvelle distro Linux
- back|track
- Les objectifs du projet
- 12 Mars 2013
- KALI Linux
- European Open-Source Meeting (SSL)
- Interview téléphonique leader developers
- Q/A

"The quieter you become, the more you are able to hear."

Sécurité Informatique Classique

VS

Sécurité Informatique Proactive

"The quieter you become, the more you are able to hear."

<< back | track 5

Sécurité Informatique Classique

Défense périmétrique avec une architecture définie "sécurisée" et systèmes IDS/IPS avec procédures de détection semi-automatisées.

Ce type de sécurité est aussi appelée:

"Sécurité Défensive"

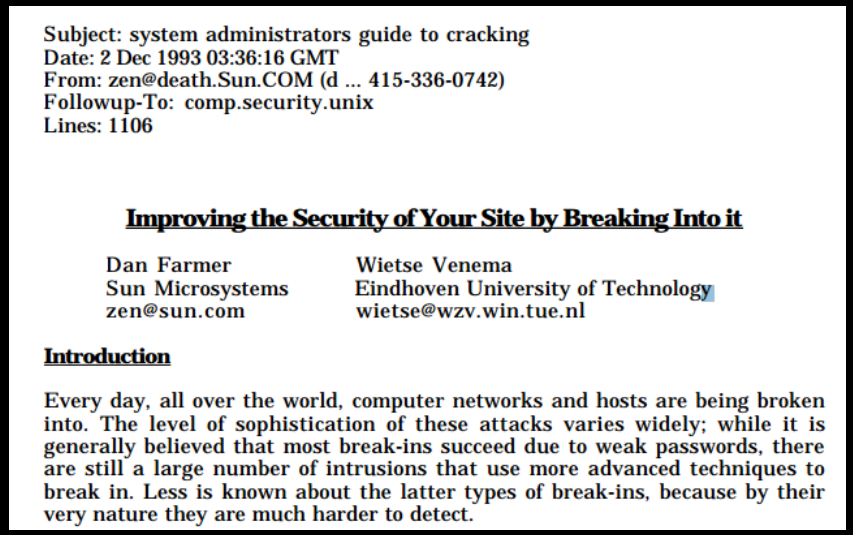
Je proportionne l'architecture de mon réseau avec un bon projet, j`achète mes appliances et les outils de protection commerciaux (généralement) avec l'espoir (ou l'arrogance?) de me tenir sécurisé et inviolable…

<< back | track 5

Sécurité Informatique Proactive

“ Improving the security of your site by breaking into it…“

Dan Farmer - 1993



Subject: system administrators guide to cracking
Date: 2 Dec 1993 03:36:16 GMT
From: zen@death.Sun.COM (d ... 415-336-0742)
Followup-To: comp.security.unix
Lines: 1106

Improving the Security of Your Site by Breaking Into it

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@wzv.win.tue.nl

Introduction

Every day, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, there are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins, because by their very nature they are much harder to detect.

<< back | track 5

Sécurité Informatique Proactive

La sécurité Informatique proactive trouve ses racines dans la nécessité de prouver l'intrusion au sein de sa propre infrastructure pour en vérifier la résistance et la non-perméabilité, en assumant le comportement d'un attaquant motivé.

Ce type de sécurité est aussi appelée:

"Sécurité Offensive"

Sur une base d'architecture de SI saine, j'installe tous mes équipements de sécurité puis je vérifie (ou je fais vérifier) la pénétrabilité et la résistance de mon système.


black hat®
<< back | track 5 r3
July 21st - 26th 2012

<< back | track 5

Backtrack v1.0 2006

- Fusion de "**Whax**" et "**Auditor**" par Mati Aharoni
- Système basé sur "**Slax**" jusqu'à la V.3
- Passage à "**Ubuntu**" depuis la V.4
- Dernière Version BT5-R3 BH Edition

"The quieter you become, the more you are able to hear."

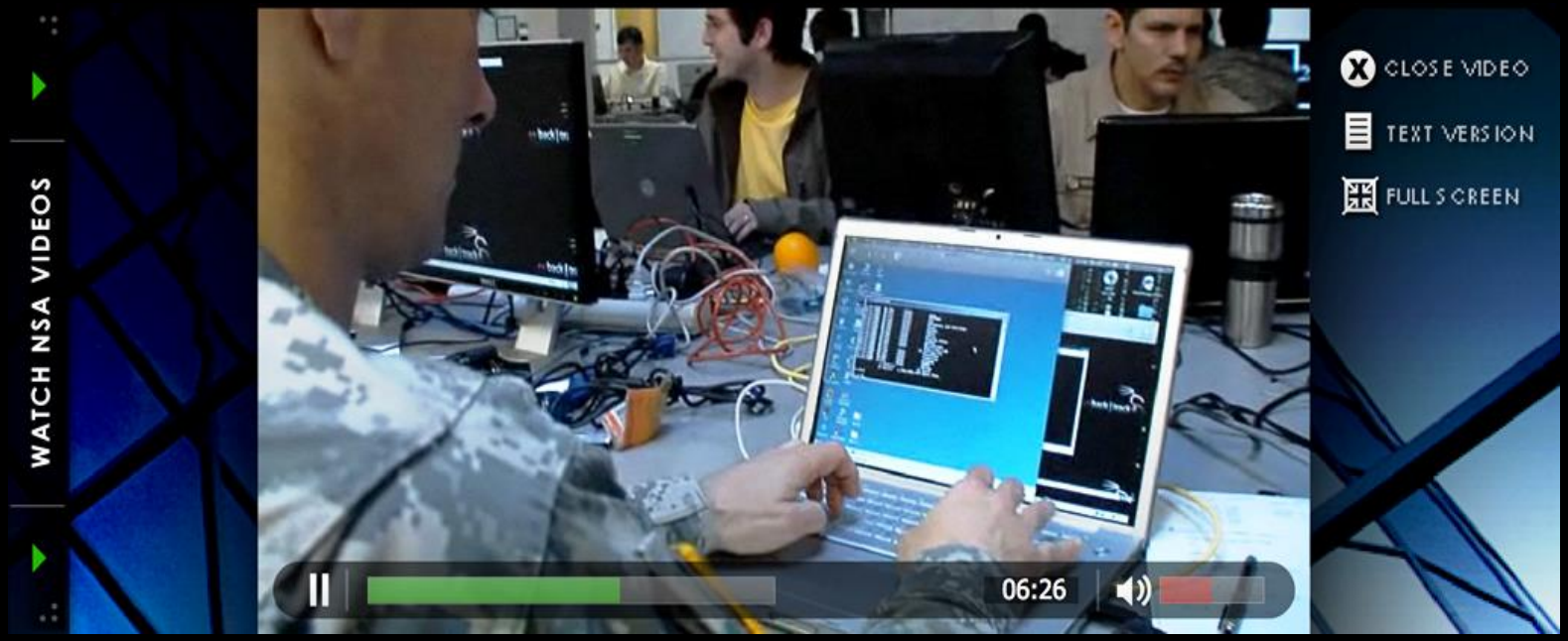
Back|Track international project

- Distribution GNU/Linux live installable pour activités d'intelligence et Penetration Test.
- Plus de 500 outils pour effectuer test de sécurité et investigation.
- Versions disponibles: i386, AMD64, ARM
- Interfaces Graphique: KDE, Gnome, Fluxbox
- Presque 6.000.000 de downloads uniques (5.997.811 le 18/10/2011) (BT5 R1)
- Utilisée par organisations militaires et agences gouvernementales

"The quieter you become, the more you are able to hear."

<< back | track 5

Back|Track international project
Defense & State Agencies (NSA)



National Security Agency

"The quieter you become, the more you are able to hear."

<< back | track 5

Back|Track international project Defense & State Agencies (NSA)

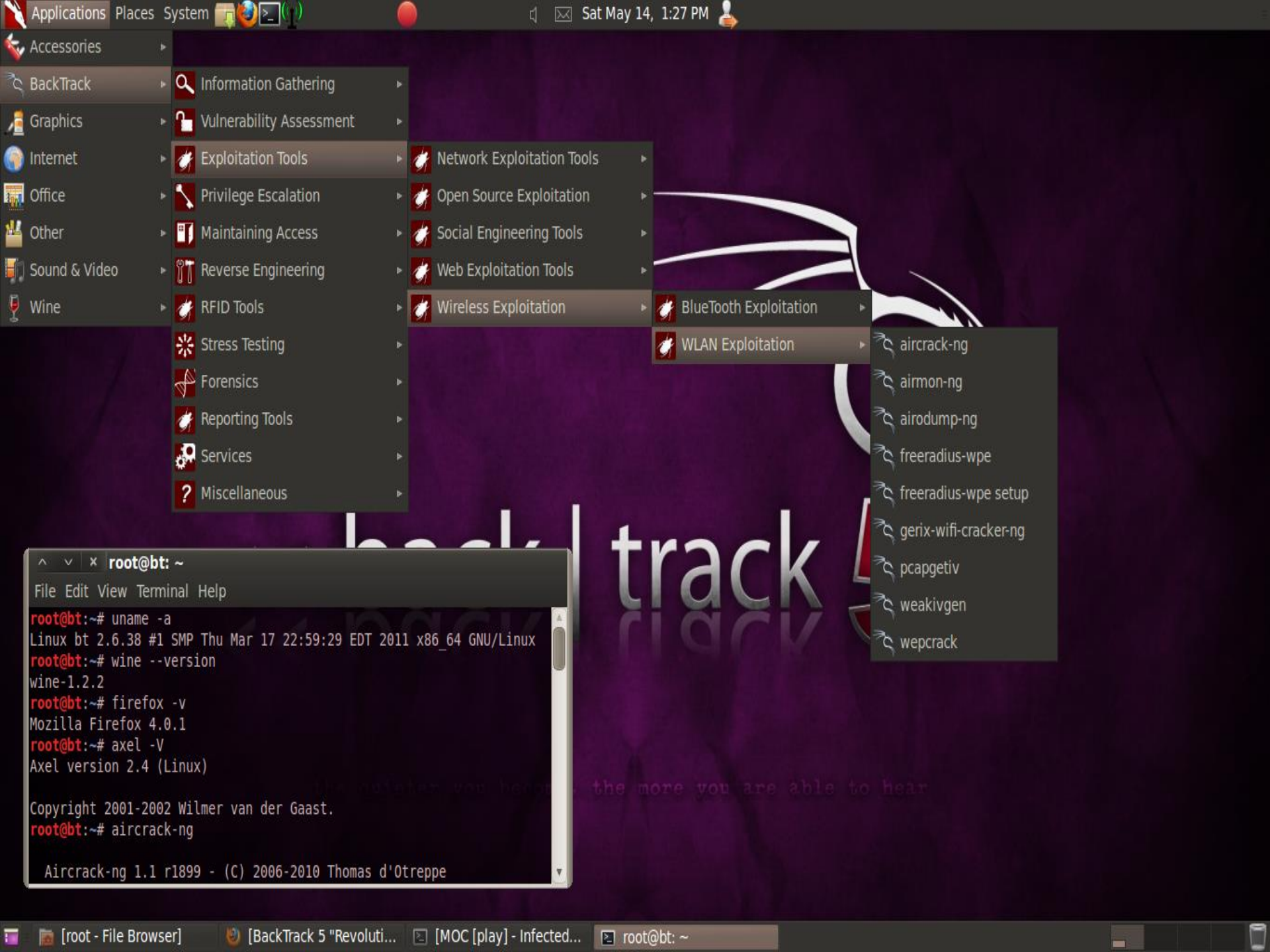
"The quieter you become, the more you are able to hear."

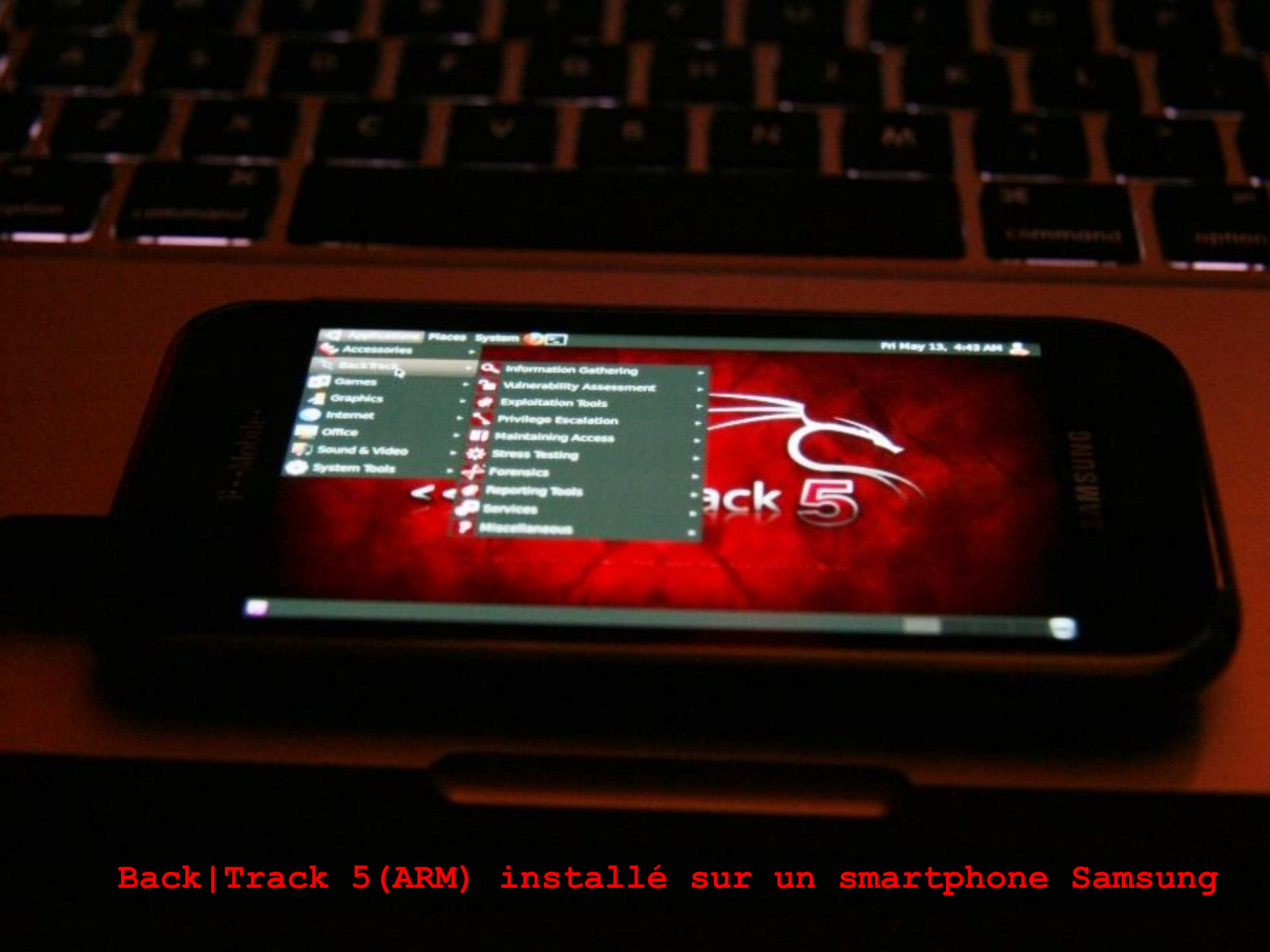
<< back | track 5

Respects des méthodologies STANDARD internationales

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP (Open Web Application Security Project)
- OSINT (Open Source Intelligence)

"The quieter you become, the more you are able to hear."


Applications
Places
System
Sat May 14, 1:27 PM
Accessories
BackTrack
Graphics
Internet
Office
Other
Sound & Video
Wine
Information Gathering
Vulnerability Assessment
Exploitation Tools
Privilege Escalation
Maintaining Access
Reverse Engineering
RFID Tools
Stress Testing
Forensics
Reporting Tools
Services
Miscellaneous
Network Exploitation Tools
Open Source Exploitation
Social Engineering Tools
Web Exploitation Tools
Wireless Exploitation
BlueTooth Exploitation
WLAN Exploitation
aircrack-ng
airmon-ng
airodump-ng
freeradius-wpe
freeradius-wpe setup
gerix-wifi-cracker-ng
pcapgetiv
weakivgen
wepcrack
root@bt: ~
File Edit View Terminal Help
root@bt:~# uname -a
Linux bt 2.6.38 #1 SMP Thu Mar 17 22:59:29 EDT 2011 x86_64 GNU/Linux
root@bt:~# wine --version
wine-1.2.2
root@bt:~# firefox -v
Mozilla Firefox 4.0.1
root@bt:~# axel -V
Axel version 2.4 (Linux)
Copyright 2001-2002 Wilmer van der Gaast.
root@bt:~# aircrack-ng
Aircrack-ng 1.1 r1899 - (C) 2006-2010 Thomas d'Otreppe
[root - File Browser]
[BackTrack 5 "Revoluti...
[MOC [play] - Infected...
root@bt: ~



Back|Track 5(ARM) installé sur un smartphone Samsung

<< back | track 5

Les objectifs du projet BackTrack

Mettre à disposition un OS complet et fonctionnel, prêt à être utilisé, pour les activités de Cyber Intelligence et les tests d'intrusion informatiques.

Open Source et gratuit pour les utilisateurs.

BackTrack popularisée aussi par...

<< back | track 5

L'initiateur du projet: Mati Aharoni

Mati (muts) est un professionnel de la sécurité informatique, qui travaille avec diverses agences militaires et gouvernementales.

Son travail quotidien:

- Recherche de vulnérabilités
- Développements d'exploits
- Pentests whitebox/blackbox

"The quieter you become, the more you are able to hear."

<< back | track 5

Les formations Offsec: Challenge/Passion/Pratique

Pentesting with BackTrack

Penetration Testing with BackTrack is an online information security training course designed for network administrators and security professionals who need to acquaint themselves with the world of offensive information security. This penetration testing training introduces the latest hacking tools and techniques in the field and simulates a full penetration test, from start to finish, by injecting the student into a diverse and vulnerable network.

MORE INFO

Metasploit Unleashed

Metasploit Unleashed is a free online information security training course that was created to fill a gap in quality documentation on the practical usage of the popular and versatile Metasploit Framework. In keeping with the open-source nature of Metasploit, we provide this resource free of charge to the information security community. Any and all donations received are donated to Hackers for Charity.

MORE INFO

Wireless Attacks

Offensive Security Wireless Attacks teaches students the base concepts of wireless networking and builds upon that foundation to conduct effective attacks against wireless networks of varying configurations. Not just for penetration testers, this course is highly recommended for anyone responsible for wireless networks. By understanding how they are attacked, administrators will know how best to protect their wireless infrastructure.

MORE INFO

Cracking the Perimeter

Cracking the Perimeter takes all of the skills acquired in the Penetration Testing with BackTrack course and further hones them by exposing students to an extremely challenging lab environment developed using actual scenarios faced by the Offensive Security team during live penetration tests. During the course, students are given an in depth examination of the vectors used by today's attackers to breach infrastructure security.

MORE INFO

Advanced Windows Exploitation

Advanced Windows Exploitation makes use of extensive hands-on material, covering such advanced topics as DEP and ASLR evasion, heap spraying, function pointer overwrites, buffer space limitations, Windows driver exploits, and creating custom hand-made shellcode. This is not an entry-level course. Experience with a debugger, previous Windows exploitation, and a intense tolerance for hard work is required.

MORE INFO

Advanced Web Attacks

Advanced Web Attacks and Exploitation takes the student deep into the realm of web application penetration testing. From mind-bending XSS attacks, to exploiting race conditions, to advanced SQL injection attacks, Advanced Web Attacks and Exploitation will broaden your knowledge of web application hacking and help you identify and circumvent various protection mechanisms in use on the web today.

MORE INFO

"The quieter you become, the more you are able to hear."


KALI LINUX

<< back | track 5

12 Mars 2013

Sortie de Kali Linux V1.0

Bien que Kali fut préparée en secret, son développement progresse à partir de maintenant au grand jour, dans des dépôts publics Git:

http://git.kali.org/

"The quieter you become, the more you are able to hear."

<< back | track 5

Pourquoi le nom Kali?

Pourquoi pas ?

- Dans l'hindouisme, la déesse du Temps, de mort et de délivrance, mère destructrice et créatrice.
- Kali est un nom sanskrit renvoyant à la notion de noirceur, d'obscurité et de dureté.
- Kali escrima est un art martial philippin.
- Backtrack est « à la retraite…» ;)

<< back | track 5

LES CHANGEMENTS

- Purge du nombre d'outils
- Migration vers Debian Wheezy
- Les paquets Debian sont maintenus via git-buildpackage, pristine-tar et les outils associés, rendant ainsi l'intégration des dernières modifications de Debian facile.
- Kali a empaqueté plusieurs centaines d'outils et entend contribuer en retour à Debian avec les principes du logiciel libre selon Debian.
- Des dépôts existent pour tous les paquets ayant été créés (ou modifiés), de même que pour le script de création des images ISO.

<< back | track 5

Plus de 90.000 downloads!

"The quieter you become, the more you are able to hear."

<< back | track 5

- Versions disponibles: KDE, Gnome, i386, AMD64, ARM
- La plupart des paquets Kali sont importés non-modifiés des dépôts Debian
- Possibilité de construire ses propres ISO Kali personnalisés (grâce à Debian live-build scripts)
- Outil de rapport de bugs en ligne « *bugs.kali.org* »

"The quieter you become, the more you are able to hear."

<< back | track 5

Applications Places Sat Jan 1, 12:12 AM root

Computer

Raspberry Pi

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# aireplay-ng -9 mon0
00:02:39  Trying broadcast probe requests...
00:02:39  Injection is working!
00:02:41  Found 5 APs

00:02:41  Trying directed probe requests...
00:02:41  0C:37:DC:85:B2:88 - channel: 1 - 'CHB-3G-2'
00:02:41  Ping (min/avg/max): 1.442ms/7.709ms/30.351ms Power: -57.00
00:02:41  30/30: 100%
```

Terminal

File Edit View Search Terminal Help

```
 +-------------------------+-------------------------+
 |      o 0 o              |        \'\/\/\/'/       |
 |             o 0         |         )======(        |
 |               o         |       .'  LOOT  '.      |
 |  |^^^^^^^^^^^^^^|l___   |      /    _||__   \      |
 |  |    PAYLOAD    |""\___, |     /    (_||_    \     |
 |  |_______________|__|)__| |    |      __||_)    |    |
 |  |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "    |
 |   = = = = = = = = = = =  |     '--------------'      |
 +-------------------------+-------------------------+


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf > uname -a
[*] exec: uname -a

Linux kali 3.0.68-kali #3 SMP Sun Mar 10 18:51:42 EDT 2013 armv7l GNU/Linux
msf >
```

KALI LINUX

The quieter you become, the more you are able to hea

root@kali: ~ Terminal

"The quieter you become, the more you are able to hear."

<< back | track 5

Kali Linux est LA SEULE distribution Linux supportée officiellement par "Rapid7" sur le projet "Metasploit"

"The quieter you become, the more you are able to hear."

<< back | track 5

www.exploit-db.com
www.explo.it

"The quieter you become, the more you are able to hear."

<< back | track 5

Exploit-DB (EDB) est un archive d'exploits et de logiciels vulnérables, avec documentations et POC.

GHDB, remote/local, WEB, DoS, Shellcodes, Papers.

Une ressource importante pour les auditeurs de sécurité, les chercheurs et les passionnés.

European Open-Source Meeting (SSL)
&
Communauté BackTrack

"The quieter you become, the more you are able to hear."

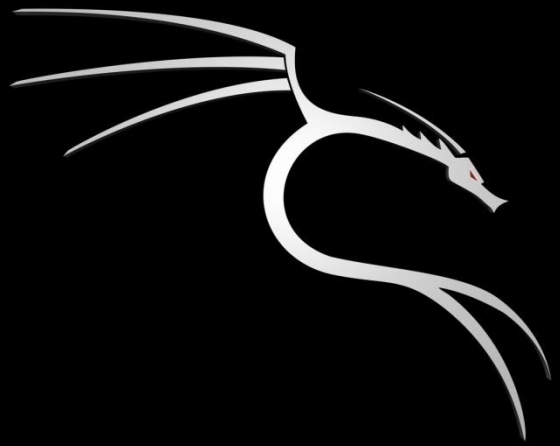
<< back | track 5

www.solutionslinux.fr

"The quieter you become, the more you are able to hear."

<< back | track 5

La communauté BackTrack



"The quieter you become, the more you are able to hear."

<< back | track 5

Leader Developers

Emanuele '*crossbower*' Acri

Emanuele '*emgent*' Gentili

"The quieter you become, the more you are able to hear."

<< back | track 5

www.phrack.org/issues.html?issue=68&id=9#article

Abusing Netlogon to steal an Active Directory's secrets — the p1ckp0ck3t

Shmeck

various

Comments

Text mode

```
I recommend all readers who have judged this article interesting, to follow
this talk, because it is a similar research, but parallel to mine.

My goal was to implement a stealth backdoor without creating new processes
or threads, while the research of Aseem focuses on the creation of threads,
to achieve the same level of stealthiness.

I therefore offer my best wishes to Aseem, since I think our works are
complementary.

For additional material on "injection of code" you can see the links
listed at the end of the document.

Bye bye ppl ;)

Greetings (in random order): emgent, scox, white_sheep (and all ihteam),
sugar, renaud, bt_smarto, cris.

------[ 8. Links and references

[0] https://secure.wikimedia.org/wikipedia/en/wiki/Ptrace
[1] http://dl.packetstormsecurity.net/papers/unix/elf-runtime-fixup.txt
[2] http://www.phrack.org/issues.html?issue=58&id=4#article
    (5 - The dynamic linker's dl-resolve() function)
[3] http://vxheavens.com/lib/vrn00.html#c42
[4] http://cymothoa.sourceforge.net/
[5] http://www.exploit-db.com/exploits/13388/
[6] http://debugmo.de/2009/04/bgrep-a-binary-grep/
[7] https://www.defcon.org/html/defcon-19/dc-19-speakers.html#Jakhar

------[ 7. Further readings
------[ 8. Links and references
```

"The quieter you become, the more you are able to hear."

<< back | track 5

I recommend all readers who have judged this article interesting, to follow this talk, because it is a similar research, but parallel to mine.

My goal was to implement a stealth backdoor without creating new processes or threads, while the research of Aseem focuses on the creation of threads, to achieve the same level of stealthiness.

I therefore offer my best wishes to Aseem, since I think our works are complementary.

For additional material on "injection of code" you can see the links listed at the end of the document.

Bye bye ppl ;)

Greetings (in random order): emgent, scox, white_sheep (and all ihteam), sugar, renaud, bt_smarto, cris.

------[8. Links and references

[0] https://secure.wikimedia.org/wikipedia/en/wiki/Ptrace
[1] http://dl.packetstormsecurity.net/papers/unix/elf-runtime-fixup.txt
[2] http://www.phrack.org/issues.html?issue=58&id=4#article
    (5 - The dynamic linker's dl-resolve() function)
[3] http://vxheavens.com/lib/vrn00.html#c42
[4] http://cymothoa.sourceforge.net/
[5] http://www.exploit-db.com/exploits/13388/
[6] http://debugmo.de/2009/04/bgrep-a-binary-grep/
[7] https://www.defcon.org/html/defcon-19/dc-19-speakers.html#Jakhar

<< back | track 5

Leader Developers

Emanuele '*crossbower*' Acri

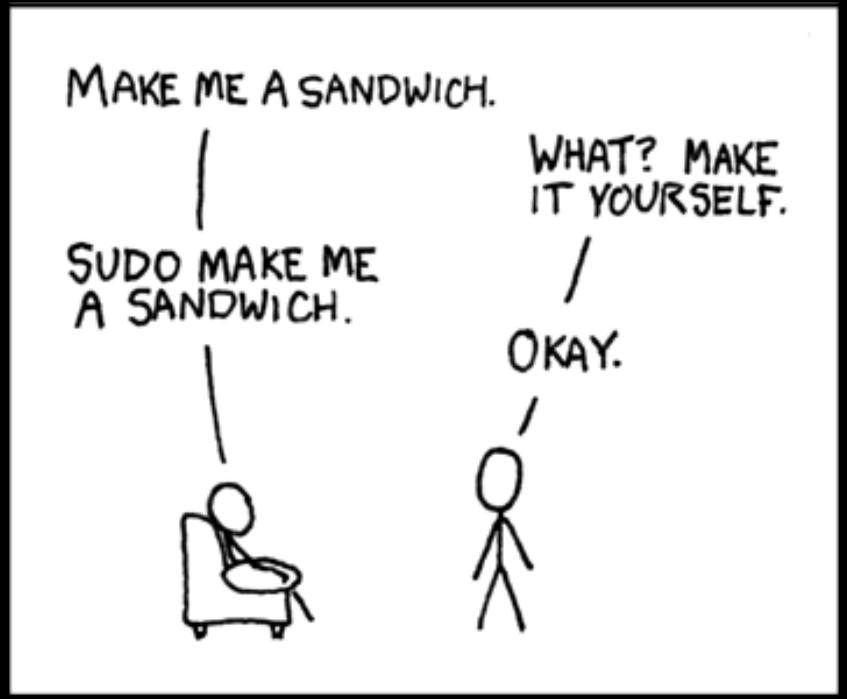
"The quieter you become, the more you are able to hear."

CONCLUSION?

"The quieter you become, the more you are able to hear."

<< back | track 5

Aujourd'hui on peut bien essayer de sécuriser et tester notre périmètre au maximum mais le point faible est, et restera toujours le même…



<< back | track 5

"Social Engineering attack because there is no patch to human stupidity..."

"The quieter you become, the more you are able to hear."

<< back | track 5

QUESTIONS?

"The quieter you become, the more you are able to hear."

Giovanni 'sug4r' RATTARO
Renaud 'action09' LEROY

europe@backtrack-linux.org

<< back | track 5

Merci !

"The quieter you become, the more you are able to hear."